CTSC
CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

LIGO

Streamlining Collaboration with InCommon and Identity Federations

Warren G Anderson, Ph.D. (LIGO)
Jim Basney, Ph.D. (CTSC)

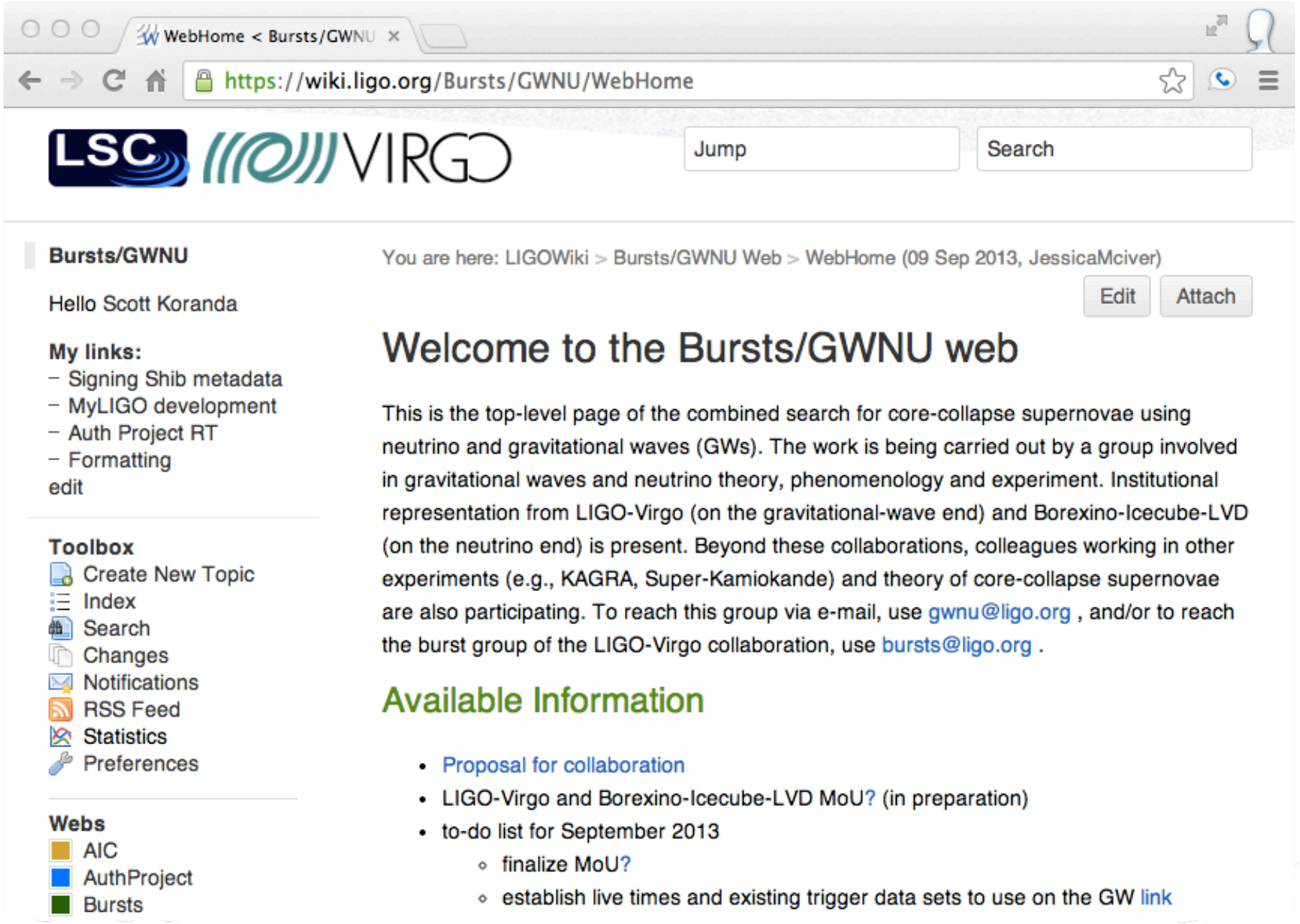
PART I - *INTRODUCTION*

"The journey of a thousand miles begins with one step."

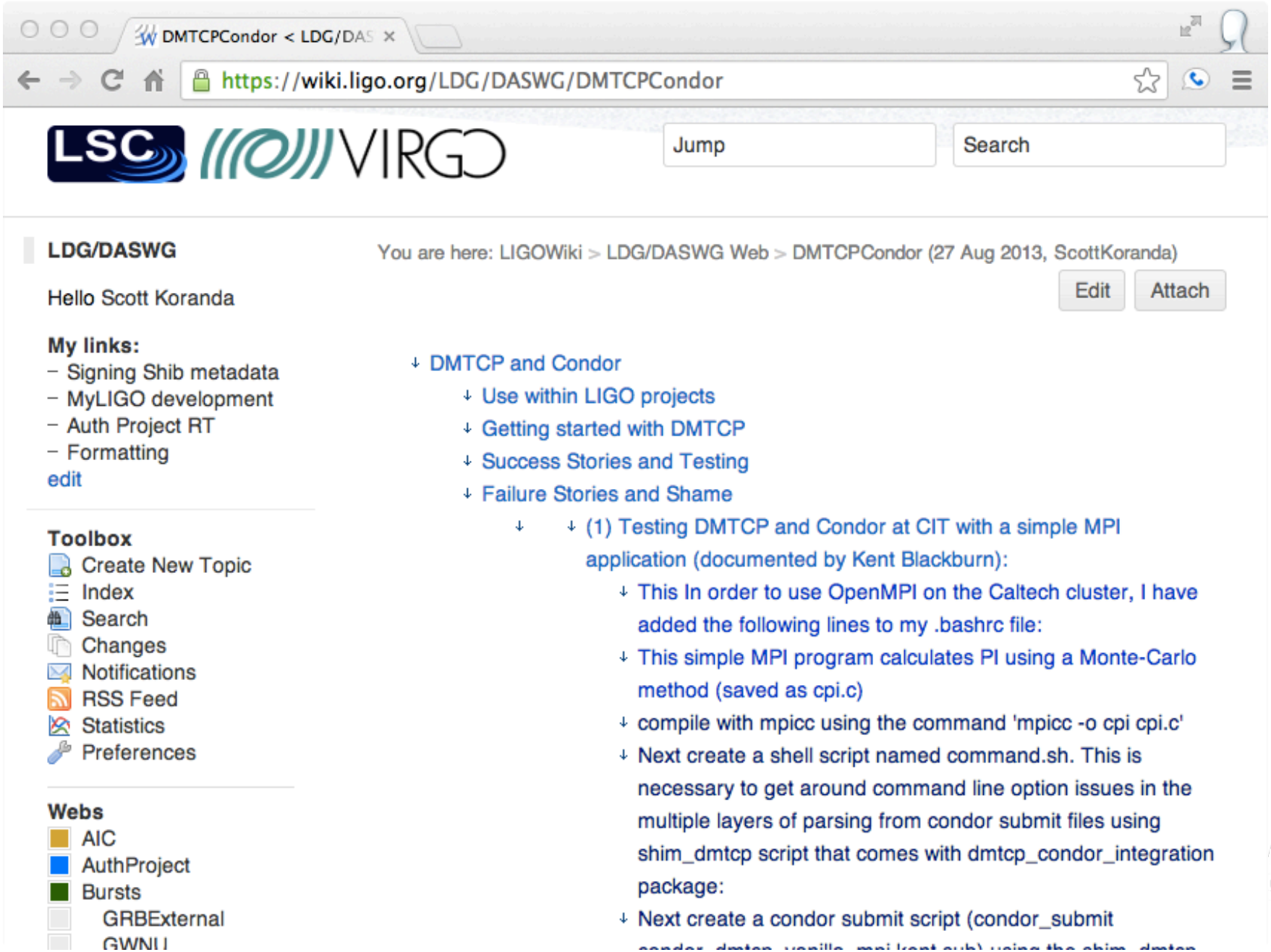
Lao Tzu

Research VOs are Collaborations

VOs Collaborate With VOs



Support Requires Collaboration



Collaboration Often Cumbersome

Too often getting access requires new identity

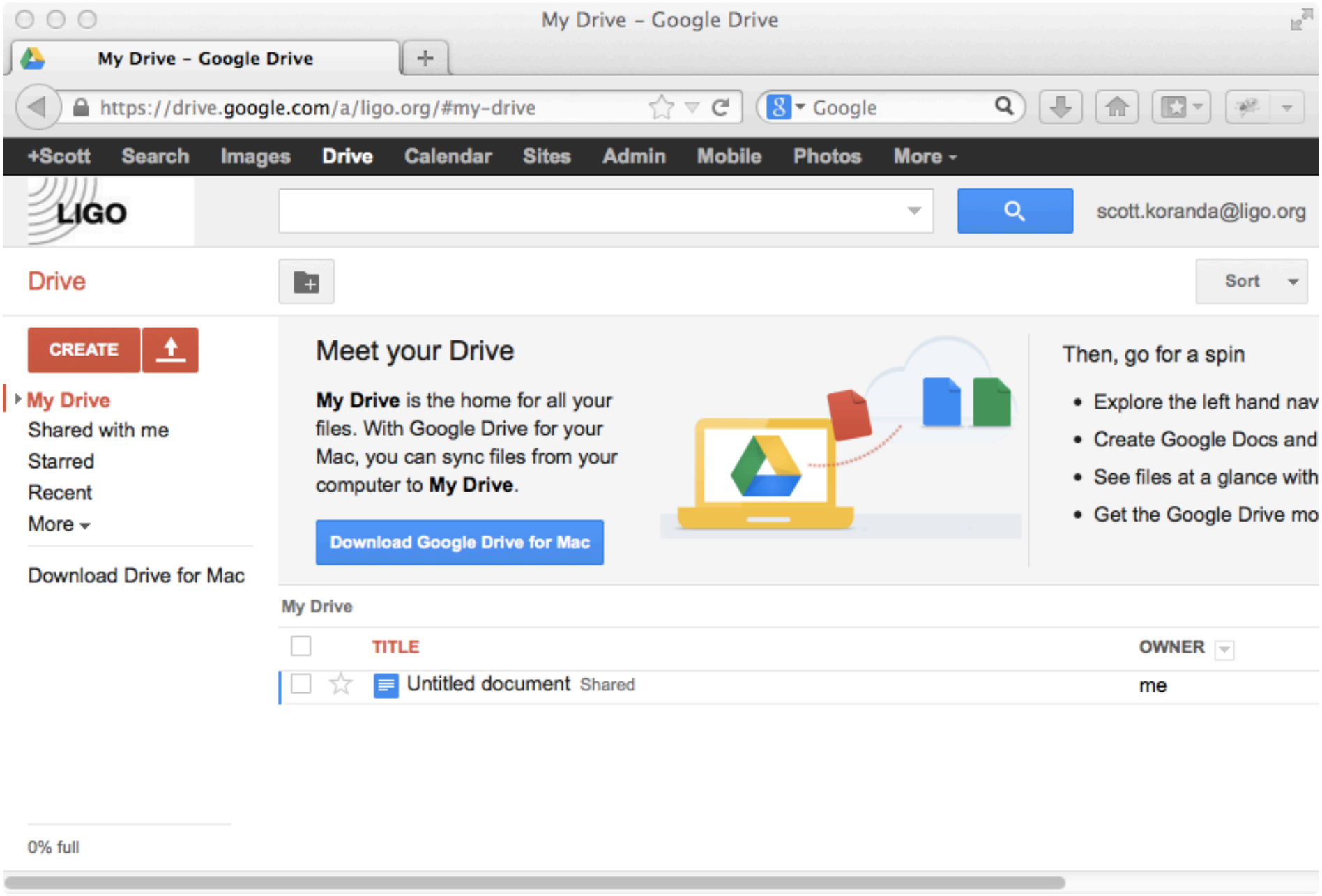
"Just click here to ask for a new account"

- May take days or weeks for new account
- Frustrates users both inside and outside VO
- Organization "leaks" accounts and access
  - Right now does your VO know who can access what and for how long?

Enabling Efficient VO Collaboration

What's a science VO to do?

Google Apps!


My Drive – Google Drive
My Drive – Google Drive
https://drive.google.com/a/ligo.org/#my-drive
Google
+Scott
Search
Images
Drive
Calendar
Sites
Admin
Mobile
Photos
More
LIGO
scott.koranda@ligo.org
Drive
Sort
CREATE
My Drive
Shared with me
Starred
Recent
More
Download Drive for Mac
Meet your Drive
My Drive is the home for all your files. With Google Drive for your Mac, you can sync files from your computer to My Drive.
Download Google Drive for Mac
Then, go for a spin
Explore the left hand nav
Create Google Docs and
See files at a glance with
Get the Google Drive mo
My Drive
TITLE
OWNER
Untitled document Shared
me
0% full

Google Apps?

Everyone just use Google!

If you can do this then do it...

- Fast to set up
- Easy for users
- Free (as in beer)
- Just works

Google Apps?

Does not fit all VOs

- Sharing documents isn't the only need
  - Also access to domain specific services and tools
- Real privacy concerns
  - Especially for international collaborations
- As VO grows do does need for infrastructure
  - Google Apps only part of a solution
  - Larger VOs driven to look more "enterprise"

Science VO IAM

VOs need Identity & Access Management plan

- Enable access to services, tools, and data
- Manage that access to support VO mission
- It's not a data curation plan...
- It's not a cybersecurity plan
- Distinct effort
  - who gets access to what, when, and why
- Federated identity should be important part of plan

PART II – *IAM IN A NUTSHELL*

"Any philosophy that can be put in a nutshell belongs there."

Sydney J. Harris

Definition - Identity

- Your electronic identity
- Information set about you
- Used for
  - authentication
    (who are you)
  - authorization
    (what allowed to do)

```
scott.koranda@ligo.org
Scott
Koranda
Scott F Koranda
14145550208
staff
PO Box 413 Milwaukee, WI
LIGOVirgoLSCMember
```

Definition - Access Management

Access Management is about who can access which online resources.

Who is allowed which privileges at which times.

```
scott.koranda@ligo.org
has privileges VIEW,
EDIT, RENAME for topic
AuthProject/WebHome in
wiki.ligo.org from
January 1, 2013 through
January 31, 2013
```

Identity & Access Management (IAM)

Most people find they collect multiple identities over time, each with its own credentials and privileges.

```
scott.koranda@ligo.org
skoranda@uwm.edu
skoranda
skoranda@gmail.com
scott_koranda@yahoo.com
scott_koranda_ligo (Skype)
skoranda000 (AIM)
6310907720 (Delta)
ScottKoranda (Foswiki.org)
skoranda (github)
scott_koranda (NYTimes)
Scott Koranda (Facebook)
```

IAM for Scientific Organizations

Focus here is IAM for scientific organizations.

A primary goal is enabling efficient and secure collaboration to support the science mission of the project.

IAM is successful for science VOs if it increases science opportunity.

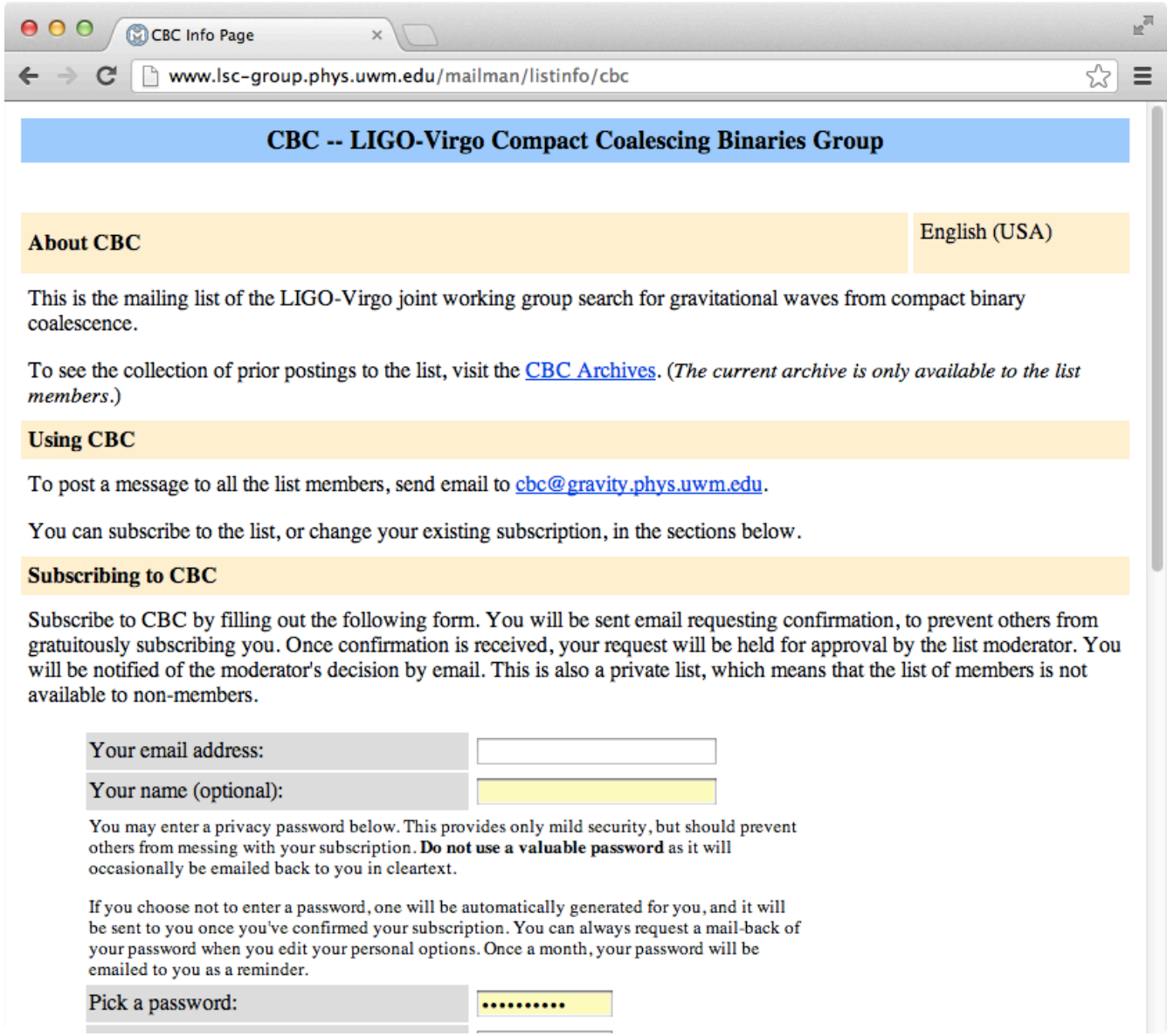
Why bother with IAM?

Larger, even medium size, science projects have tendency to evolve organically rather than by design.

And the user experience often shows it…

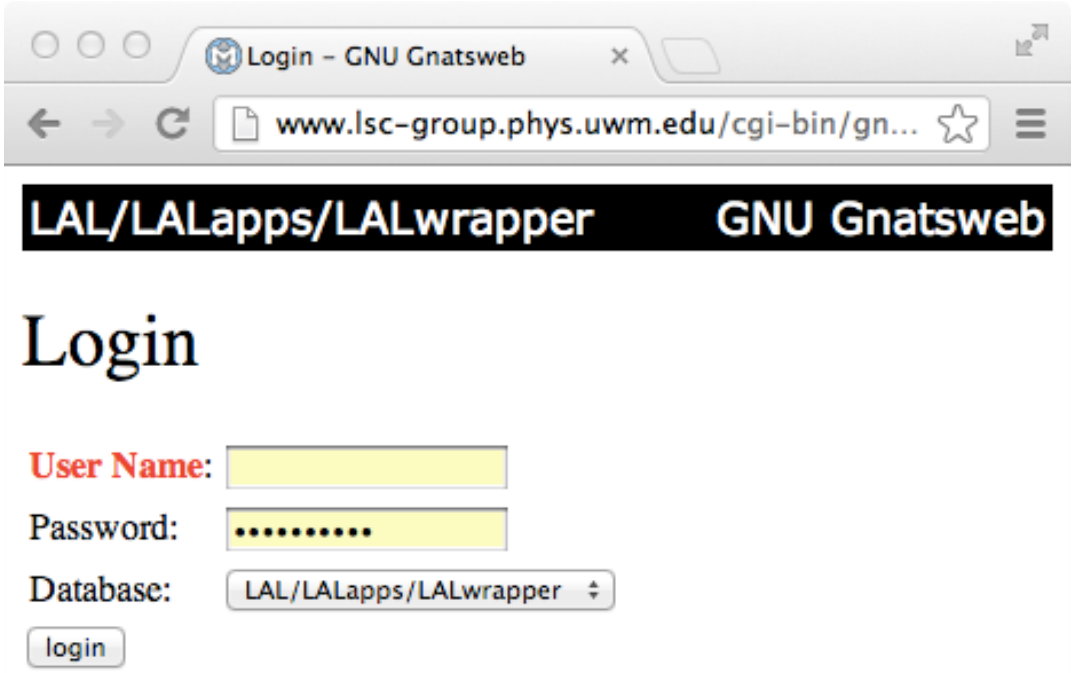
Begins innocently enough…

"We need an email list to make it easier to communicate. Let's deploy mailman."


CBC Info Page
www.lsc-group.phys.uwm.edu/mailman/listinfo/cbc
CBC -- LIGO-Virgo Compact Coalescing Binaries Group
About CBC
English (USA)
This is the mailing list of the LIGO-Virgo joint working group search for gravitational waves from compact binary coalescence.
To see the collection of prior postings to the list, visit the CBC Archives. (The current archive is only available to the list members.)
Using CBC
To post a message to all the list members, send email to cbc@gravity.phys.uwm.edu.
You can subscribe to the list, or change your existing subscription, in the sections below.
Subscribing to CBC
Subscribe to CBC by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. Once confirmation is received, your request will be held for approval by the list moderator. You will be notified of the moderator's decision by email. This is also a private list, which means that the list of members is not available to non-members.
Your email address:
Your name (optional):
You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. Do not use a valuable password as it will occasionally be emailed back to you in cleartext.
If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options. Once a month, your password will be emailed to you as a reminder.
Pick a password:

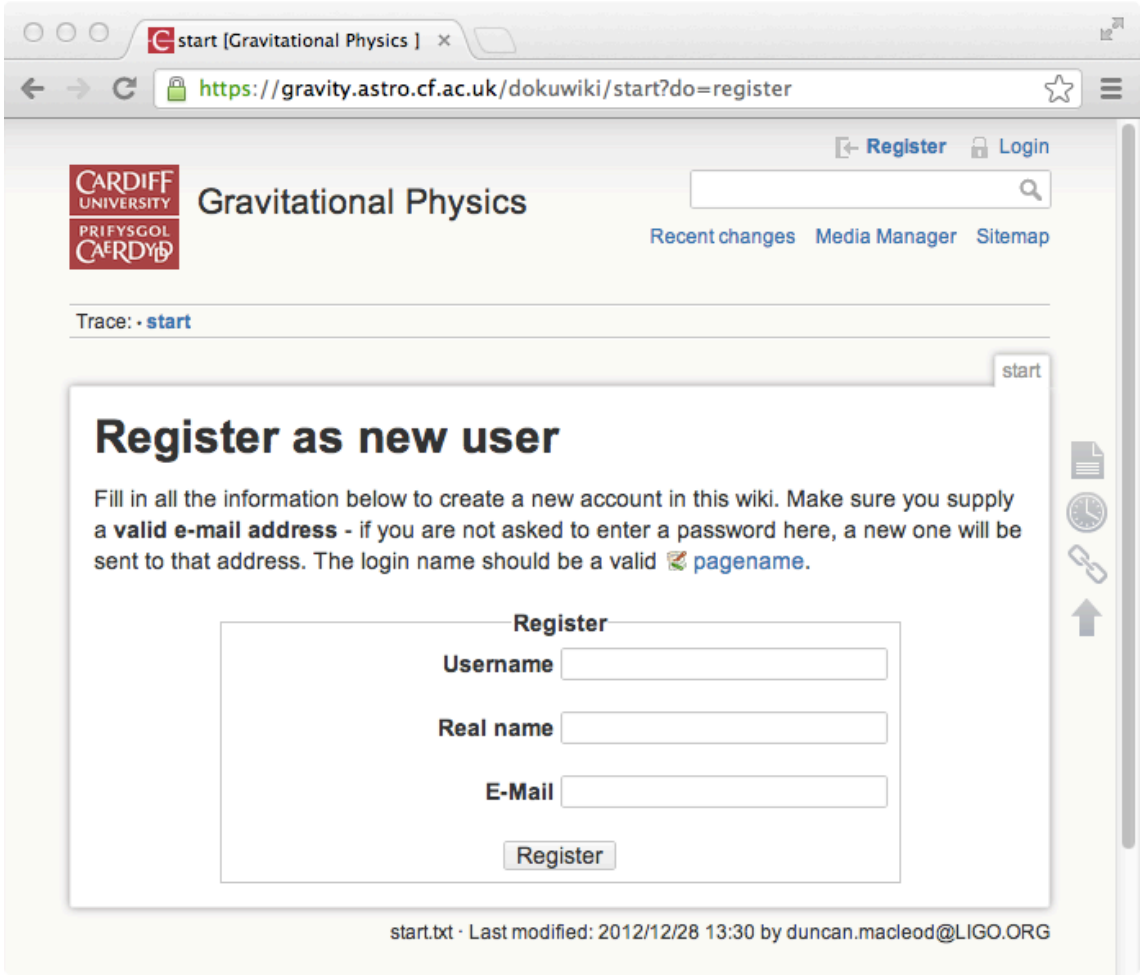
More tools follow…

"We need a bug tracking system to track all these issues!"



Still more tools...

"Editing HTML is too hard. We need a wiki."



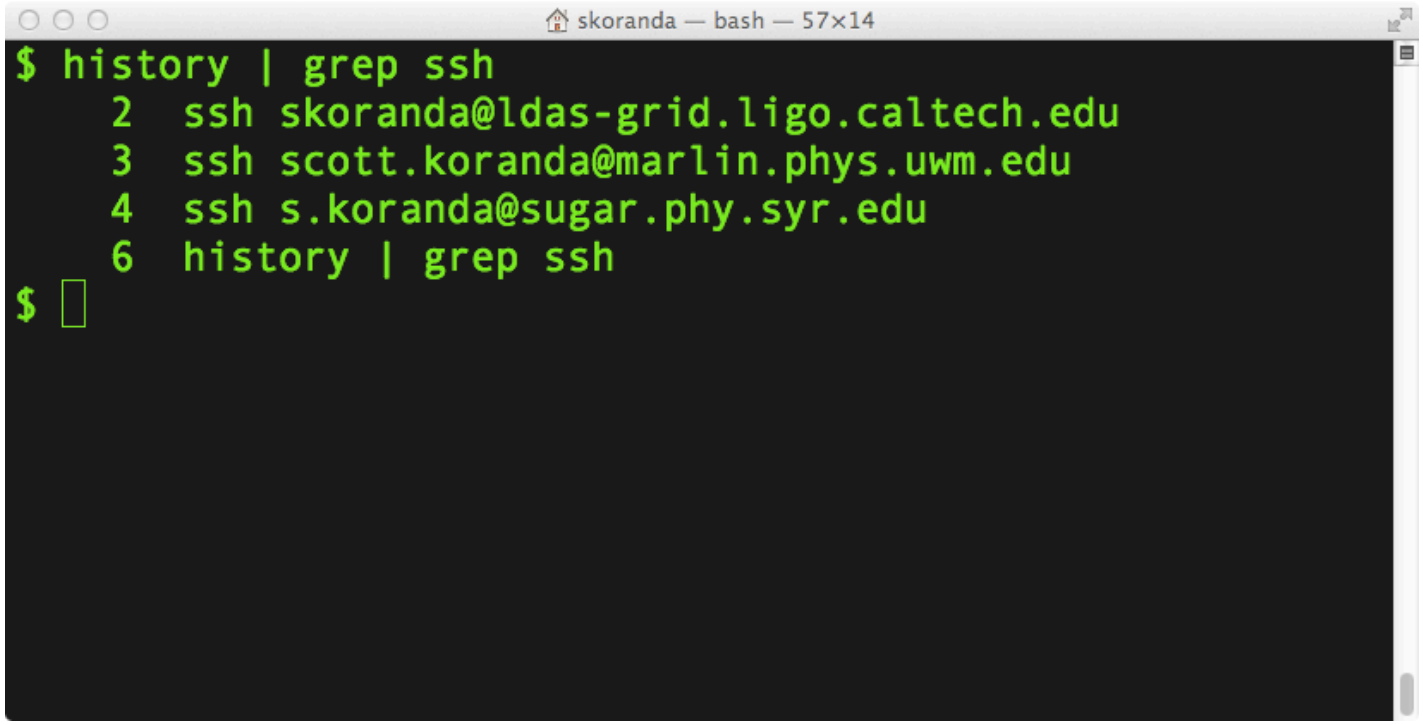
Geographic Issues

Diverse groups makes the issue worse.

“We’re not used to Moin, our lab uses Twiki”
“What’s Twiki? Our university uses Dokuwiki”
“Dokuwiki is too complicated, we use MediaWiki”
“I don’t like MediaWiki, so I wrote my own!”

Command Line Tools

This is not just a “port 80/443” problem…

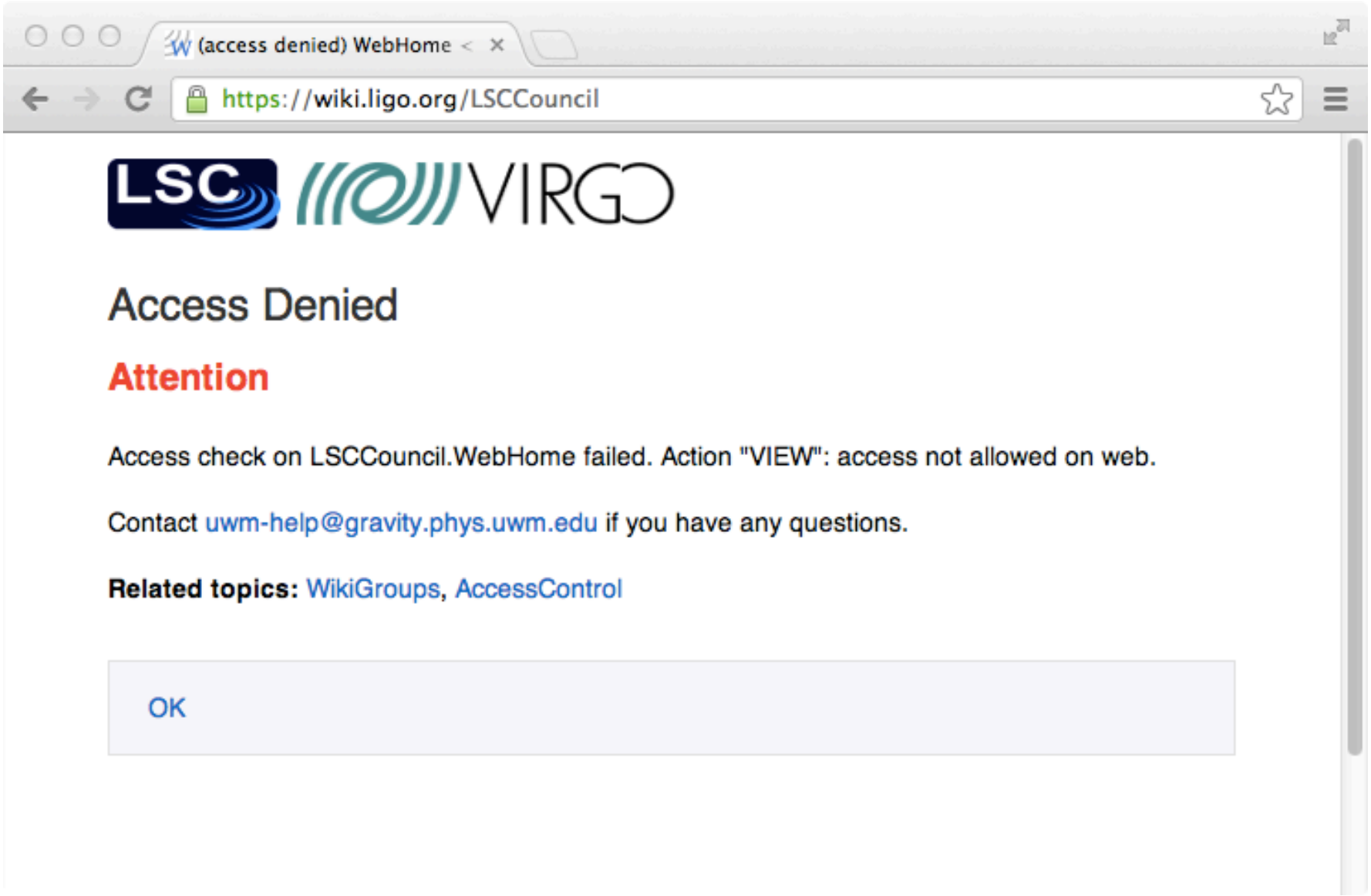


Access Management

Science VO management structure generally much flatter than Enterprise or Higher Ed.

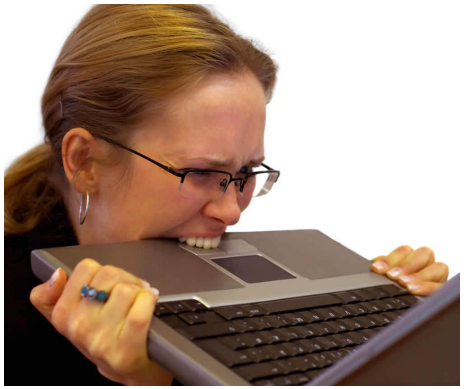
Eventually access privileges are no longer “flat.”

Some things some people can see or do…
…other things other people can see or do.


(access denied) WebHome
https://wiki.ligo.org/LSCCouncil
LSC
VIRGO
Access Denied
Attention
Access check on LSCCouncil.WebHome failed. Action "VIEW": access not allowed on web.
Contact uwm-help@gravity.phys.uwm.edu if you have any questions.
Related topics: WikiGroups, AccessControl
OK

Users Frustrated

- Eventually the burden is too high on users.
  - Too many accounts/logins/passwords.
  - Too many places to manage them.
- Drives insecure online behavior.
- Collaboration efficiency suffers.



Copyright unknown

Organizational Dysfunction

"I need a list of all people in the collaboration!"

- No such list exists
- List is not up to date
- List is inaccessible to people that need it

Organizational Dysfunction

From: admin@bigproject.org
To: users@bigproject.org
Subject: Fwd: where do I login?

Anybody know who this person is? Should she have an account?

> From: jane.scientist@university.edu
> To: admin@bigproject.org
> Subject: where do I login?
>
> I just joined Big Project and was told that you could help me get
> an account?

Organizational Dysfunction

From: jane.scientist@univeristy.edu
To: admin@bigproject.org
Subject: Fwd: minutes from last meeting

Please remove me from this list. I have not been a part of Big Project for over 2 years now!

> From: dyoung@somewhere.edu
> To: users@bigproject.org
> Subject: minutes from last meeting
>
> The minutes from the last meeting are attached. Sorry about
> the size. I don't know how to make the imported diagrams
> any smaller. Let me know if your email can't handle attachments
> more than 2 gigabytes.

IAM for Science

What makes IAM for science projects unique?

- Mixture of web and command line tools.
- Often geographically distributed.
- Often decentralized organizational structure.
- Often fewer lines of authority.
- Underfunded and not enough people resources.
- “Let’s just do it and get it done” culture.

Smart and technology savvy people +
little structure = infrastructure “challenges”

IAM for Science

Good news is that there is help:

- Technology **can** help.
- Good open source standards-based tools with strong communities available.
- Flexible, loosely coupled design goes long way.
- Leverage experience from other organizations.
  - especially campuses

IAM for Science

Bad news is that there is no silver bullet:

- Technology can only do so much.
- Policy drives the technology.
- Organizations need to articulate policies that can be implemented and expressed by the tools.
- Scientists do not like to spend time thinking through and enumerating the fine details of policy.
- Physicists particularly bad because they want to abstract the problem and find universal expressions.

Resulting policy is complex and ugly.

IAM for Science

Need to begin policy discussions early in parallel with technology design.

Drive conversations with use cases.

Iterate quickly, stand up demonstration services, help busy scientists focus on policy questions.

PART III - *IAM Model Components*

"Divide each difficulty into as many parts as is feasible and necessary to resolve it."

Rene Descartes

IAM Components

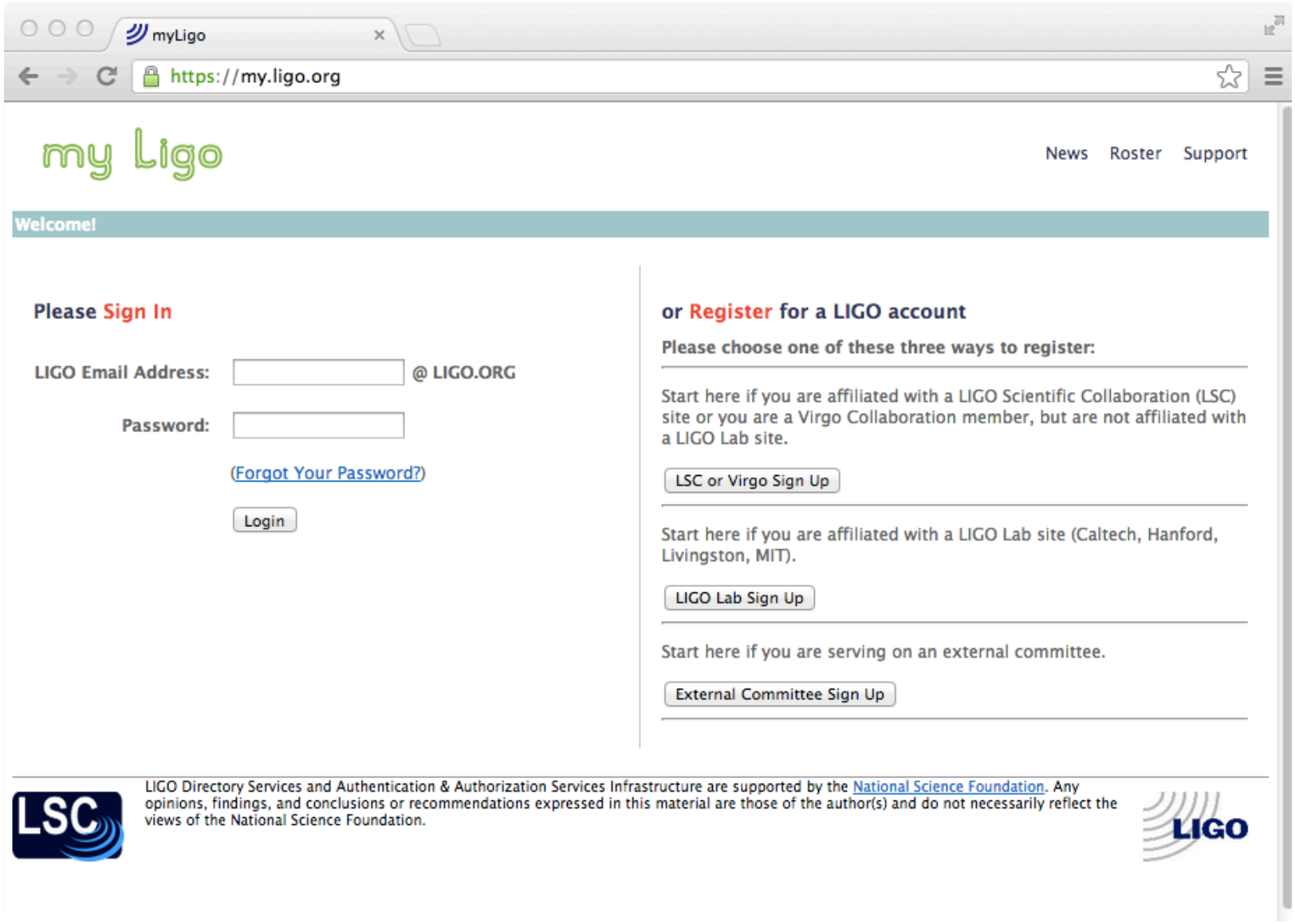
- User registry
- Directory
- Authentication store
- Identity provider
- Service providers
- Group, role, and privilege manager
- Attribute authority

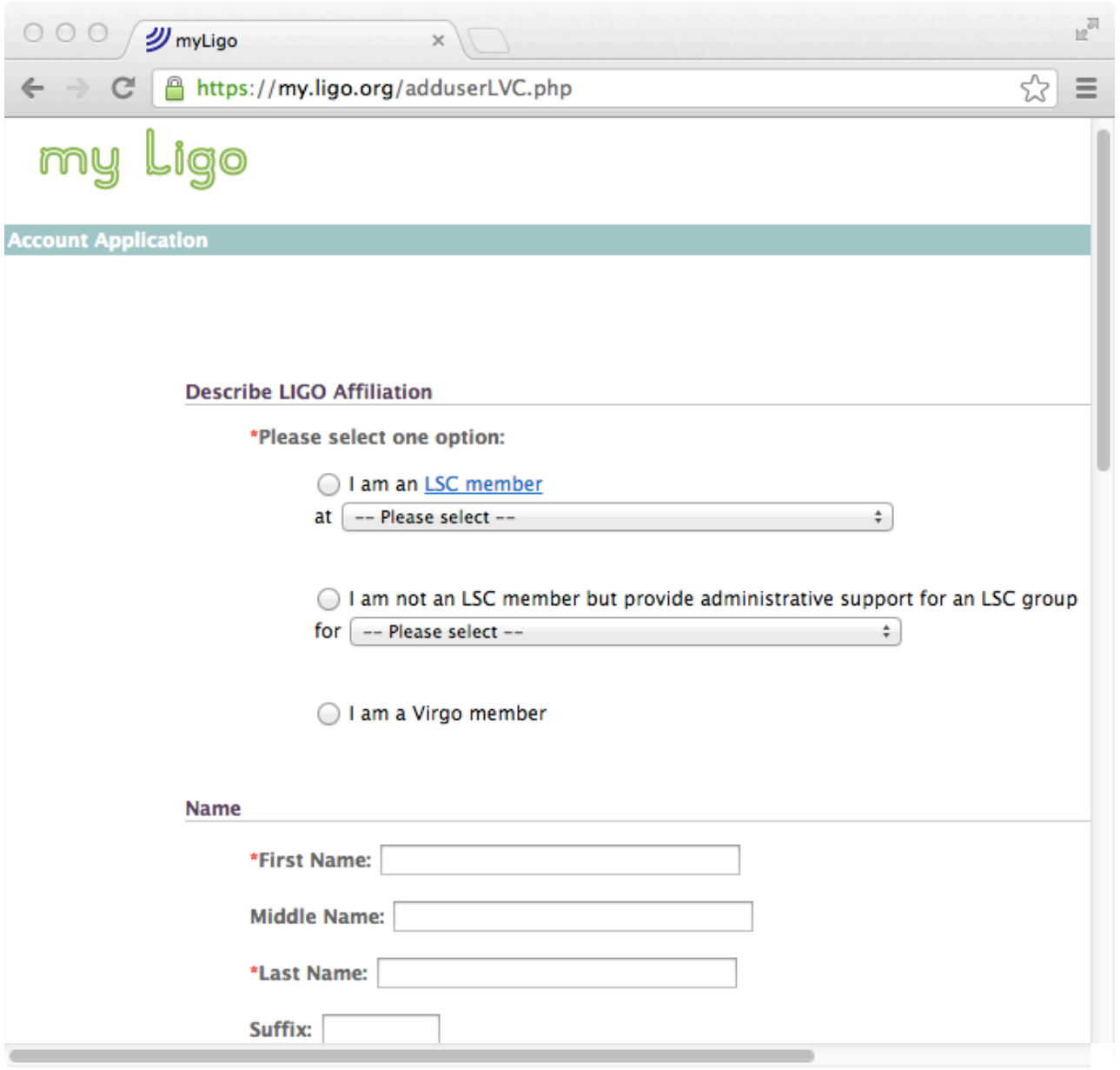
IAM Components

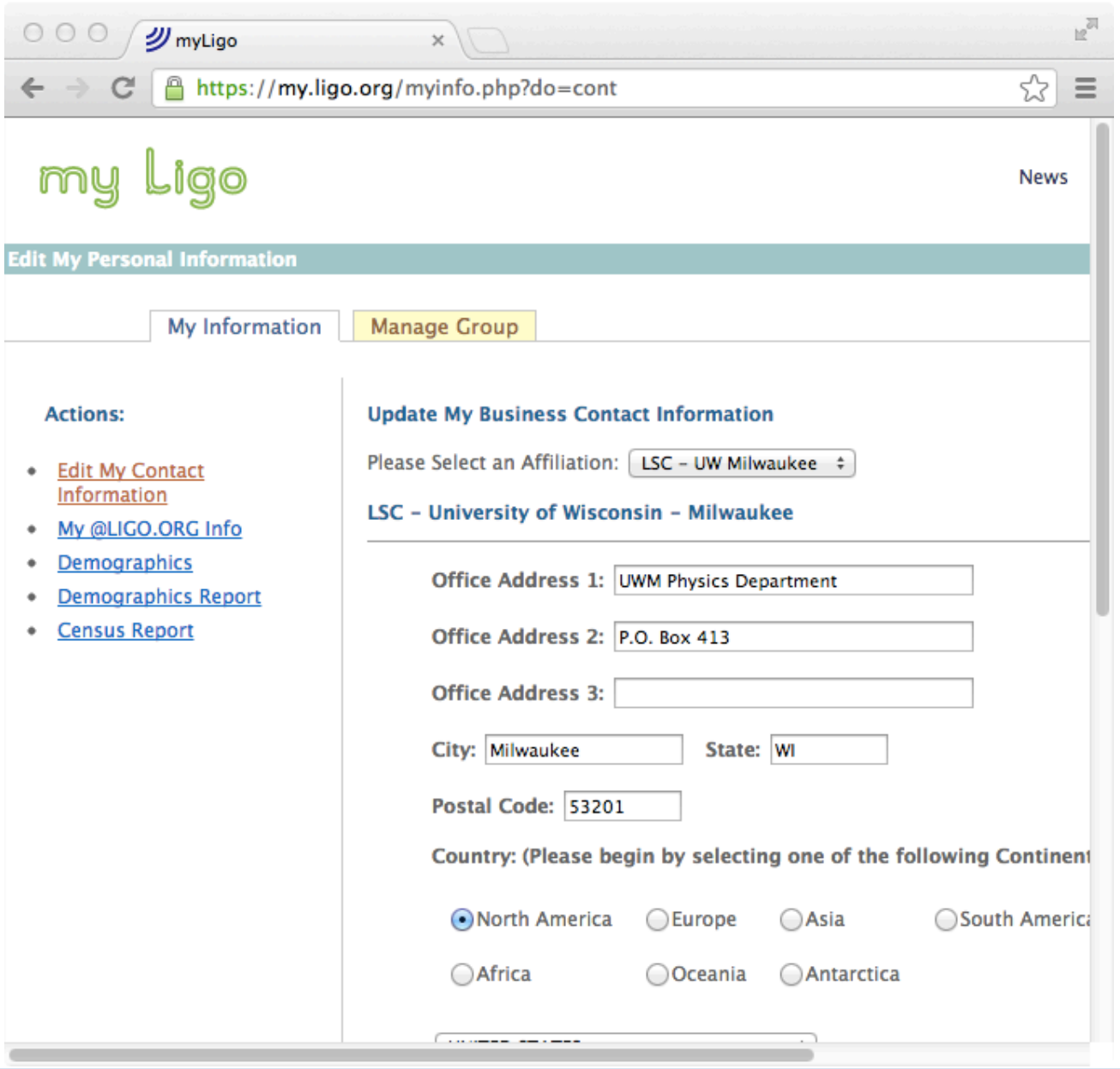
- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: User Registry

- Holds records of users or members
- Portal for users to self-manage identity
- Portal for credential (password) management
- Enrollment or “onboarding” new members
- Management of “offboarding”
- Also often reporting functions
- Also often interface into other components


myLigo
https://my.ligo.org
my Ligo
News
Roster
Support
Welcome!
Please Sign In
LIGO Email Address:
@ LIGO.ORG
Password:
(Forgot Your Password?)
Login
or Register for a LIGO account
Please choose one of these three ways to register:
Start here if you are affiliated with a LIGO Scientific Collaboration (LSC) site or you are a Virgo Collaboration member, but are not affiliated with a LIGO Lab site.
LSC or Virgo Sign Up
Start here if you are affiliated with a LIGO Lab site (Caltech, Hanford, Livingston, MIT).
LIGO Lab Sign Up
Start here if you are serving on an external committee.
External Committee Sign Up
LSC
LIGO Directory Services and Authentication & Authorization Services Infrastructure are supported by the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
LIGO


myLigo
https://my.ligo.org/adduserLVC.php
my Ligo
Account Application
Describe LIGO Affiliation
*Please select one option:
I am an LSC member
at -- Please select --
I am not an LSC member but provide administrative support for an LSC group
for -- Please select --
I am a Virgo member
Name
*First Name:
Middle Name:
*Last Name:
Suffix:


myLigo
https://my.ligo.org/myinfo.php?do=cont
my Ligo
News
Edit My Personal Information
My Information
Manage Group
Actions:
Edit My Contact Information
My @LIGO.ORG Info
Demographics
Demographics Report
Census Report
Update My Business Contact Information
Please Select an Affiliation: LSC - UW Milwaukee
LSC - University of Wisconsin - Milwaukee
Office Address 1: UWM Physics Department
Office Address 2: P.O. Box 413
Office Address 3:
City: Milwaukee
State: WI
Postal Code: 53201
Country: (Please begin by selecting one of the following Continent
North America
Europe
Asia
South America
Africa
Oceania
Antarctica

User Registry Design

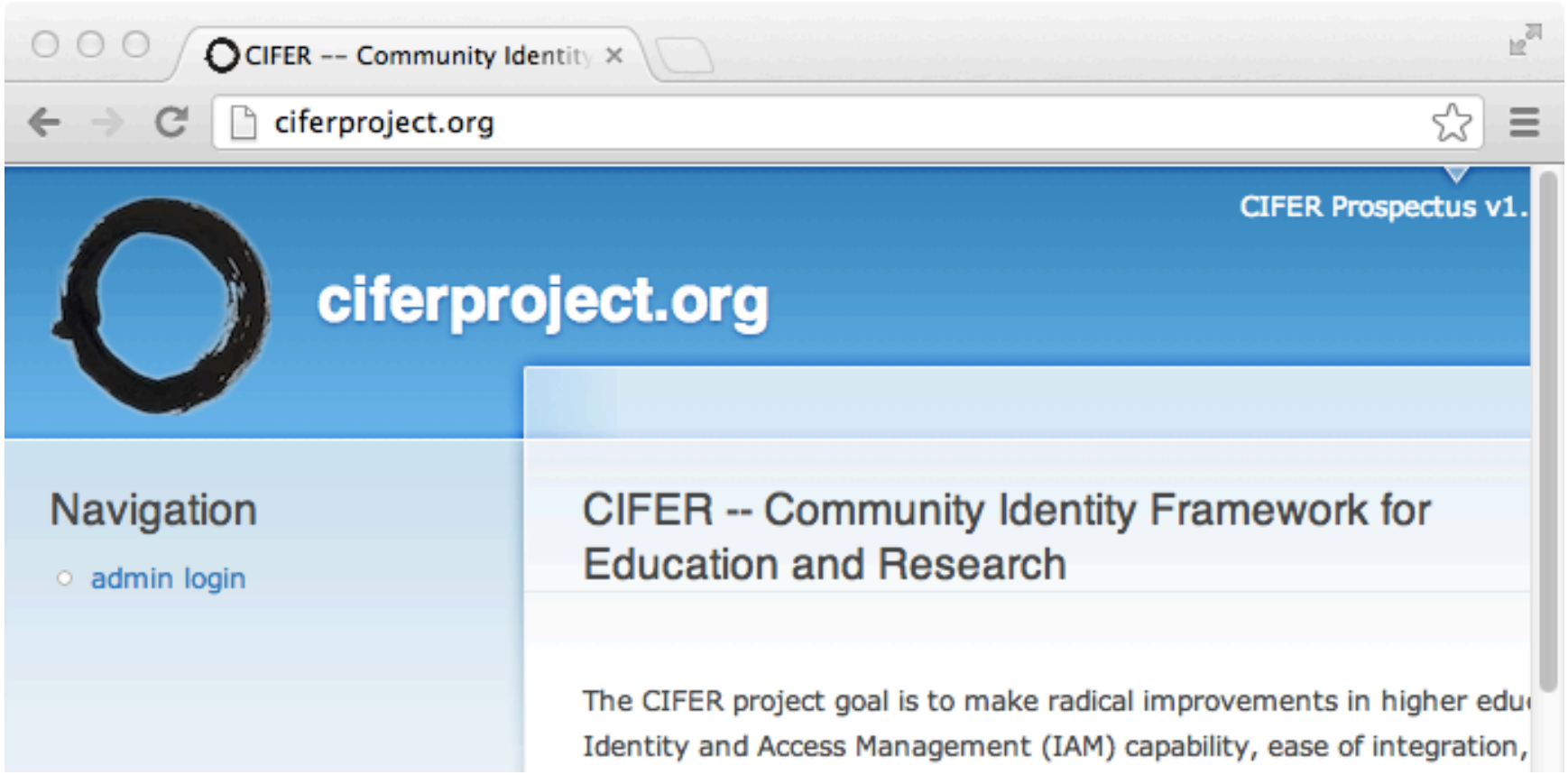
Design?

Are there not all-in-one tools to download and use?

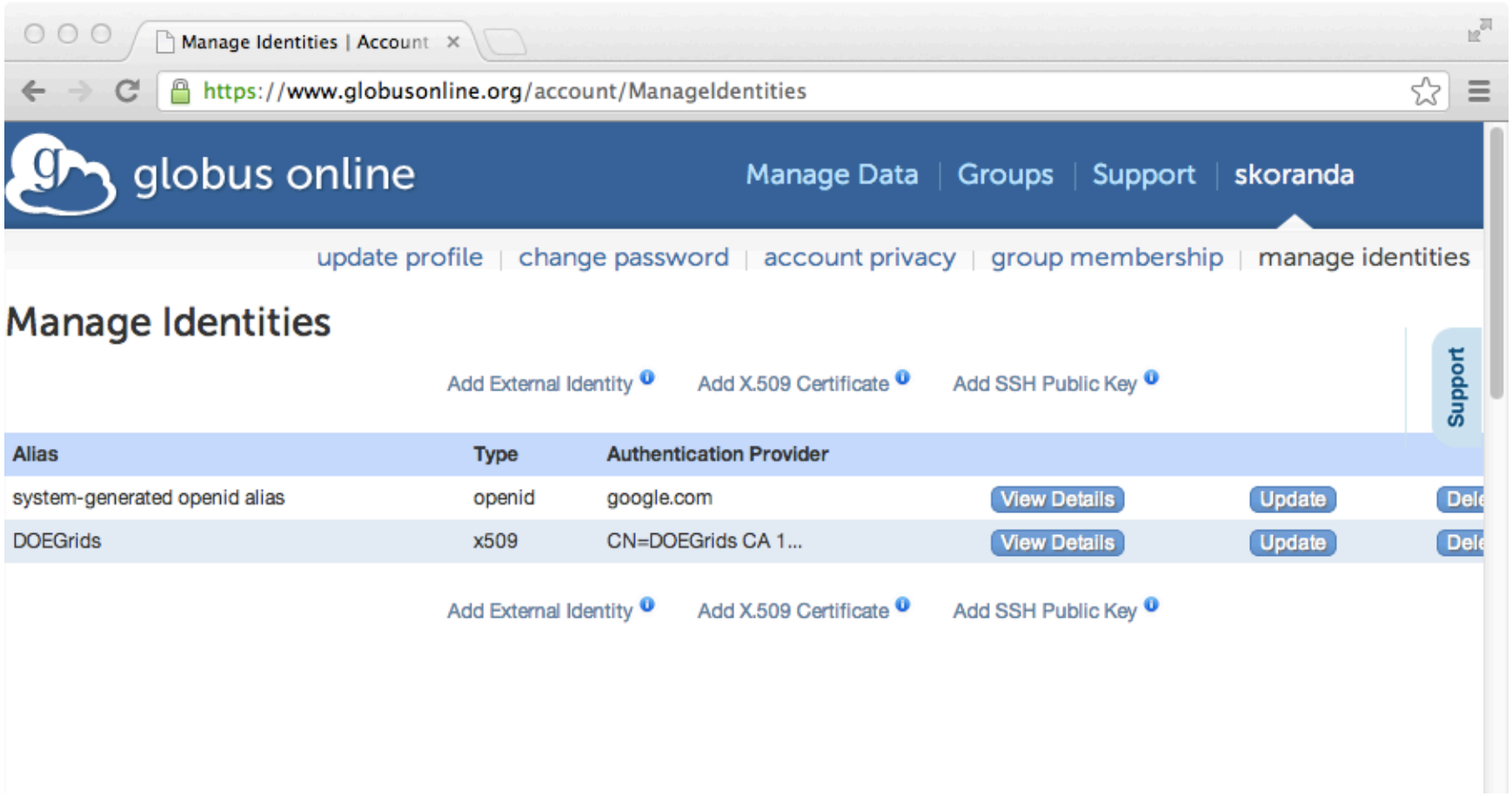
No (mostly).
Existing enterprise solutions too heavyweight and inflexible for science organizations.

LIGO currently using homebrewed solution.

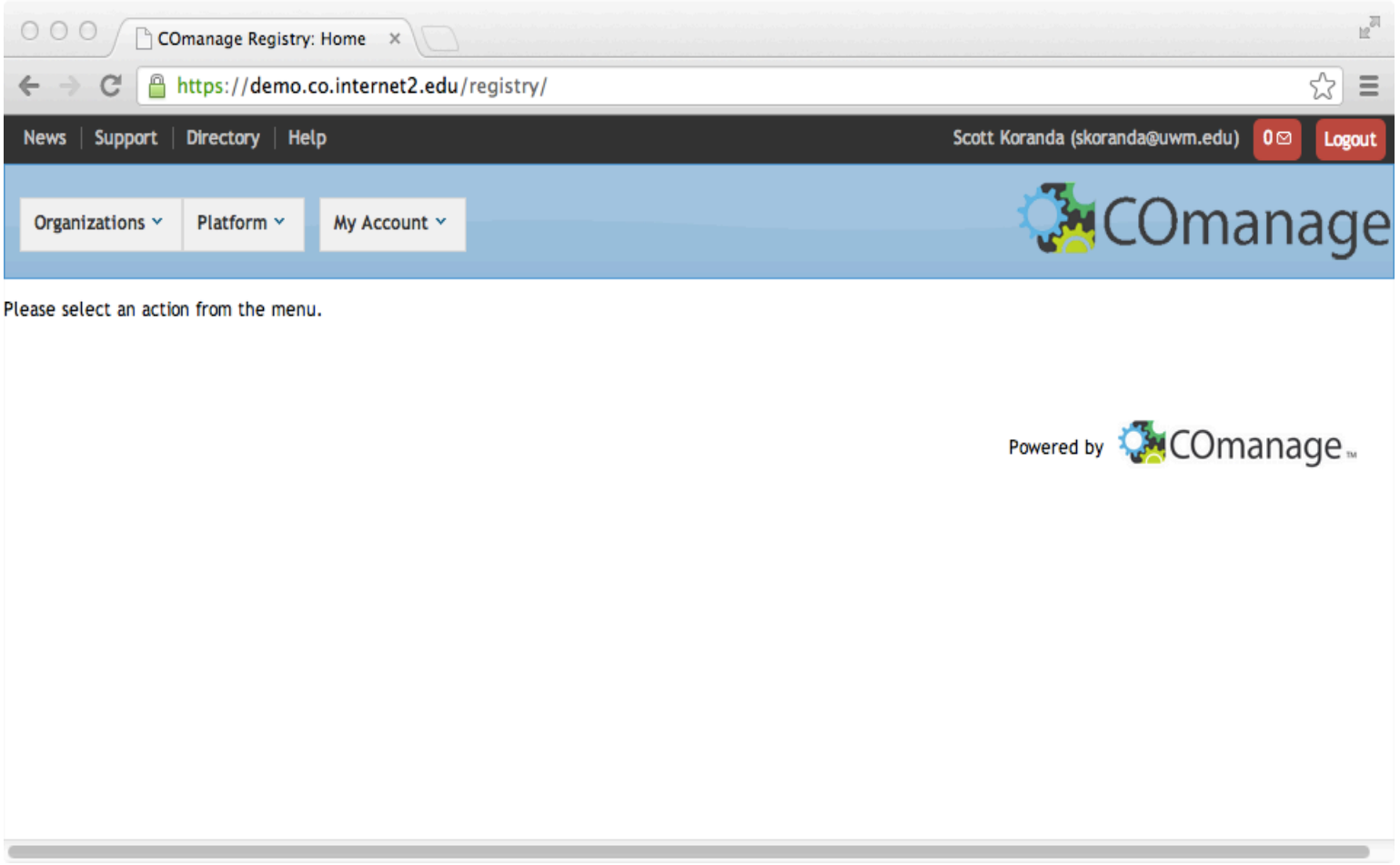
Projects to Watch



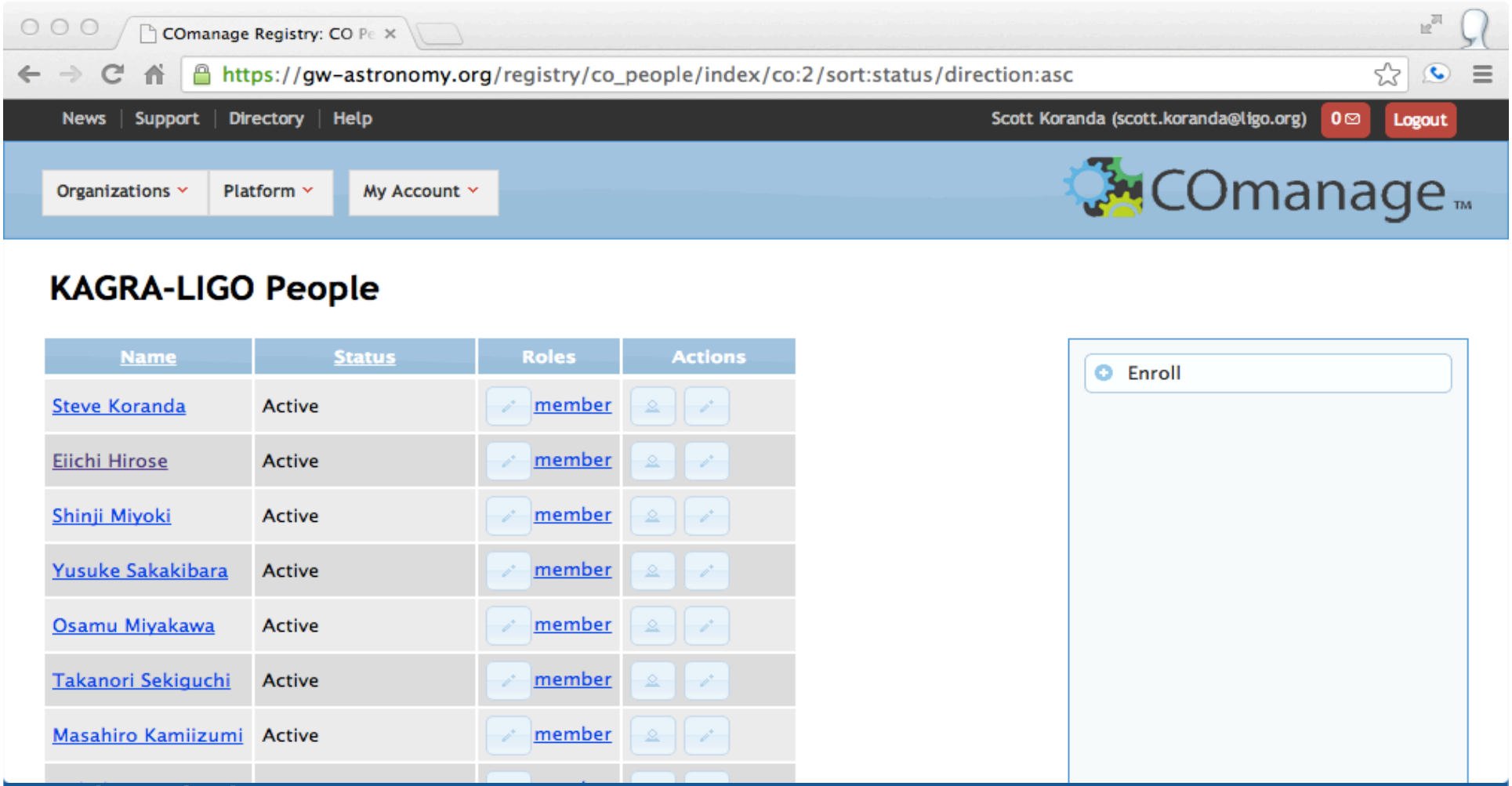
Projects to Watch



Projects to Watch



LIGO Uses COmanage



COmanage

Collaborative Organization Management

- A collaboration management platform.
- Joint project with Internet2 and iPlant.
- NSF funded.
- Supports flexible enrollment and management for federated identities.
- Provisions into attribute authority.

Collaboration Management Platforms

- COmanage (I2, LIGO, iPlant)
- OpenConext from SURFnet (NL)
- Many federations host CMP for VOs:
  - SWiTCH (CH)
  - GakuNin (JP)
  - Perun (CZ)
- Globus Online (?)

User Registry Design

Data types - What data will be stored?

Data Store - What backend data store?

Onboarding – How do new users get registered?

Offboarding – How to decommission accounts?

Reporting - What summary or metadata is needed?

User Registry Design
Data Types

What data does your project need?

- givenName
- familyName (sn)
- common name (cn)
- displayName
- preferredName
- honorific
- suffix
- mail
- mailForwardingAddress
- mailAlternateAddress
- address
- telephone
- eduPersonPrincipalName
- eduPersonOrgDN
- eduPersonAffiliation
- eduPersonEntitlement
- isMemberOf
- title
- openID
- uid
- gid
- ...

User Registry Design
Data Types

Only collect and store the data you need to accomplish the organization's mission.

Do not collect data because you "might use it someday".

Instead, design flexibility to add data types as needed.

User Registry Design
Data Types

Be sure to look at the eduPerson LDAP schema

Other resources:

- Other science projects
- CIFER, Kuali IdM, COmanage
- Your campus IT staff

User Registry Design
Data Types

Whether your registry *provisions* (is a source of) identity or *consumes* (federated) identity affects which data types to collect and store.

User Data Registry
Data Store

First question is usually SQL or LDAP?

SQL:

- More flexibility—create the tables you need.
- Integrates easily with MVC web frameworks.
  - model, view, controller
  - Django, CakePHP, Catalyst

LDAP:

- More standards—leverage existing schemas.
- Easy replication for redundancy.
- Easy integration with large number of tools.
  - pam_ldap for integration into shell

User Data Registry
Data Store

SQL or LDAP?

For small projects with limited IAM needs LDAP more likely for bootstrapping infrastructure.

For larger projects use both SQL and LDAP:

- SQL as the primary data store.
- Reflect into LDAP for replication, consumption by other tools including attribute stores.

User Registry Onboarding

Onboarding: how people enter into the IAM infrastructure.

- Usually coming new into the project.
- Sometimes returning to the project.
- May have different policies:
  - per person affiliation (faculty, staff, student, ...)
  - per organization unit
  - as project grows and matures

User Registry Offboarding

Offboarding: how people leave the IAM infrastructure.

- Always last part considered and designed!
- Usually involves decrease in privileges over time.
- May have different policies …
  - … per person affiliation (faculty, staff, student, ...)
  - … per organization unit
  - … as project grows and matures

“We need postdocs to have read and write permissions to the paper database for one year after they leave the project.”

User Registry Reporting

As size of project grows management will ask for increasingly complex views of the user registry.

Demographics, especially in the US, important to funding agencies.

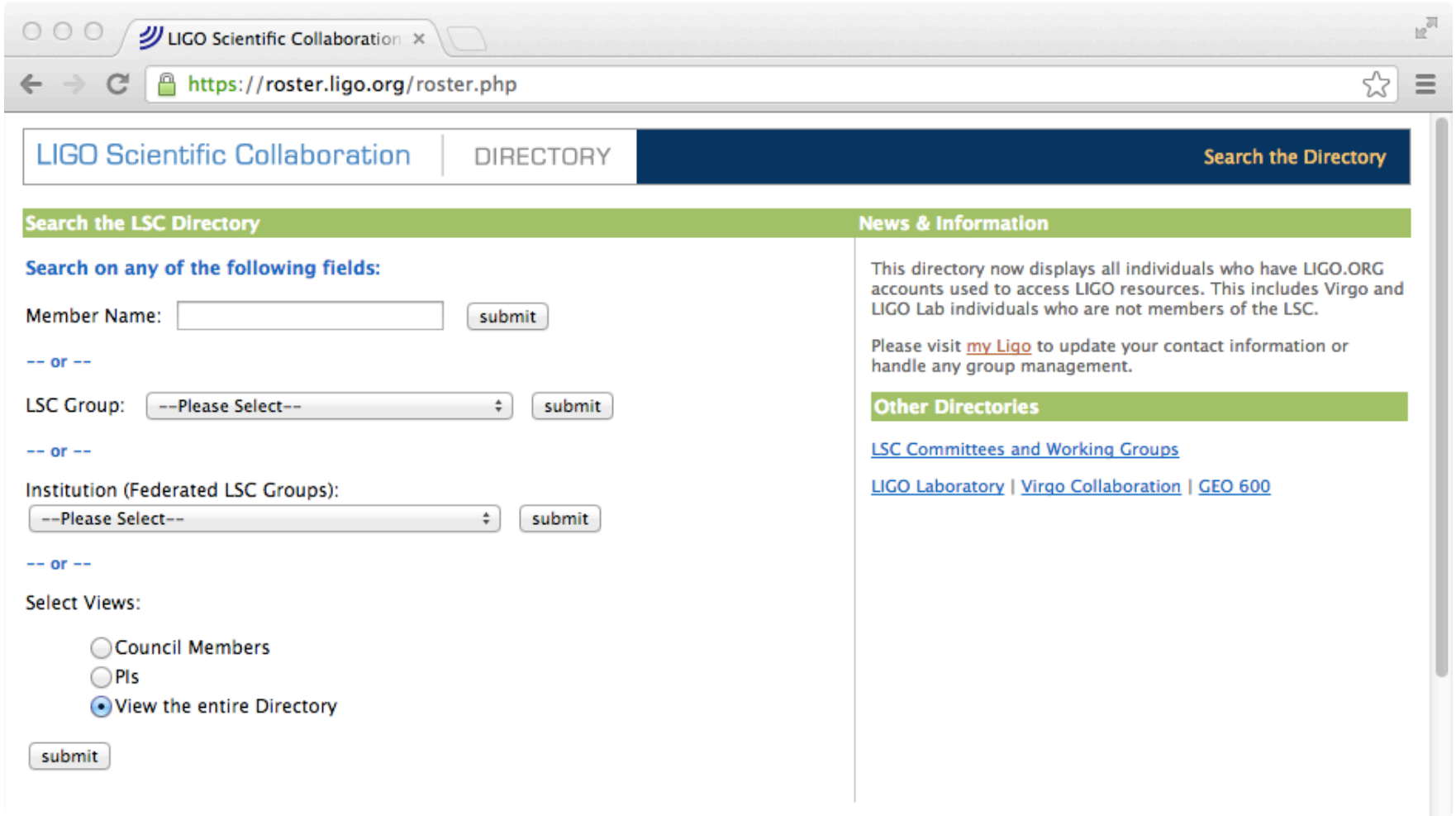
“How many female graduate students joined the project between 2010 and 2012?”

IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: Directory

Directory/Roster often first reporting from registry.



Directory/Roster

Although a “view” of the registry consider making a distinct component.

- Use a separate data store.
- Provisioned by the registry.
- Only provision subset data needed.

Help protect against PII (Personally Identifiable Information) leaks.

LIGO uses stand-alone openLDAP instance.

IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: Authentication Store

If you provision identity and with it an identifier (login) and a credential (e.g. password) used for authentication you need an authentication store.

Usual candidates:

- SQL
- LDAP
- Kerberos KDC
- Active Directory
- Shadow files

Authentication Store

Choice for authentication store depends on:

- Tools and services that need to leverage it.
  - web apps, shells, thick client, ...
- Organizational security tolerances.
  - Can passwords go over the network?
  - Over protected channels?
- Operational team experience and depth.

LIGO Authentication Store

LIGO chose Kerberos

- MIT implementation.
- Single master KDC with many slave replicas.
- Standard ports (88) and 80/443
  - Firewall traversal out of hotels for example.
- Integrated with DNS
  - Clients need no special configuration.
- Use web interface to manage password.
  - More friendly for most users.
  - Some users use command line.

LIGO Authentication Store

Kerberos principal is the primary LIGO identifier

- albert.einstein@LIGO.ORG
- LIGO.ORG is the Kerberos realm.
- LHO (soon LLO, CIT) have their own realms.
- Use cross-realm trust configuration for smooth integration.

Authentication Store

Especially with SSO, credentials are “keys to the kingdom.”

Get input from a real security expert!

IAM and security complimentary but distinct.

- Security officer has skills, training, and experience IAM architects should leverage.

Cultivate a working relationship early in design phase with your security expert.

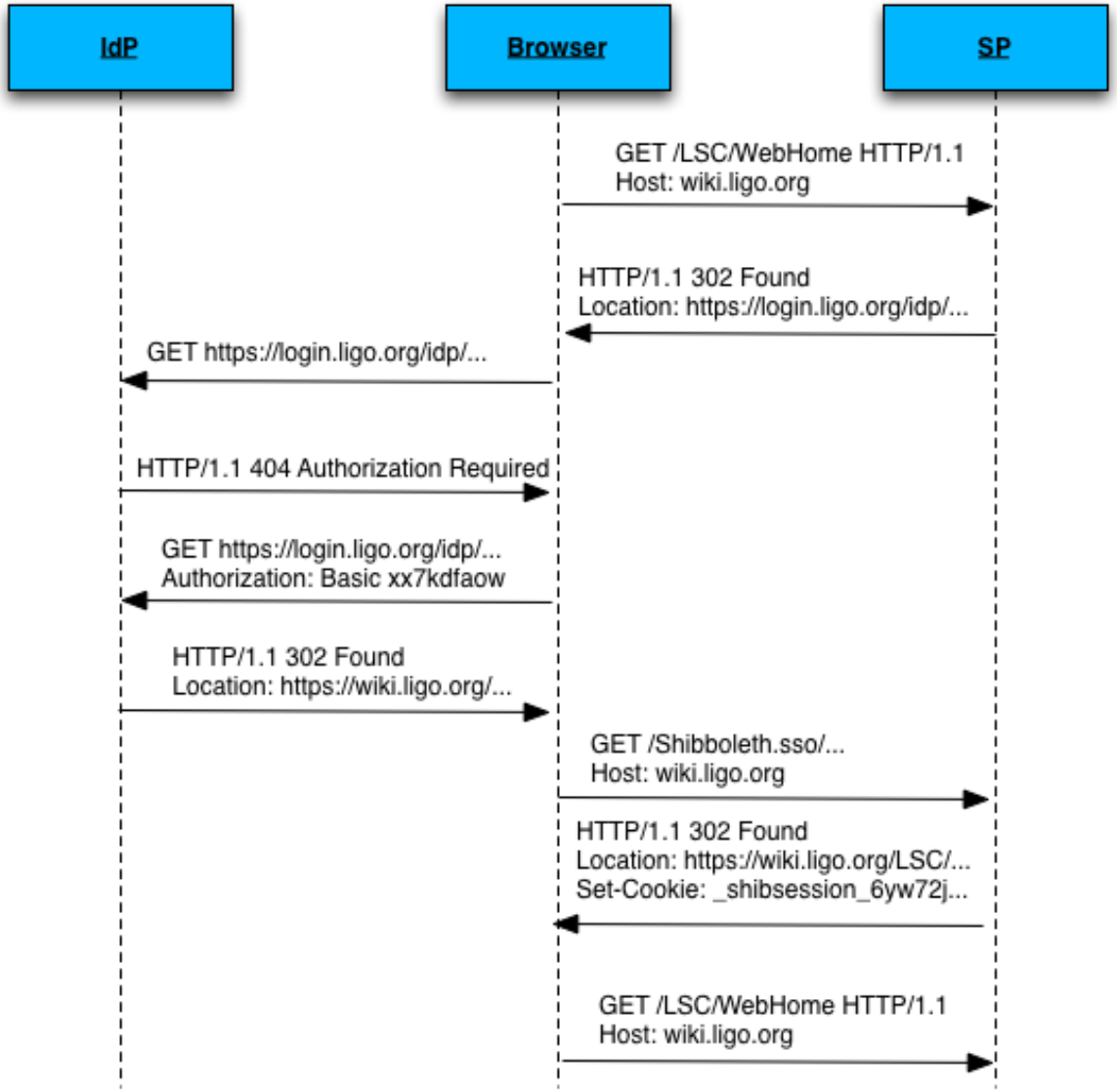
IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: Identity Provider

Identity Provider (IdP) asserts identity:

- To a third-party service provider (SP).
- Usually after an authentication event.
- Usually across a security or identity domain.
  - Still useful concept within an identity domain.
- Most often used in web context.
  - But the concept applies more generally.


IdP
Browser
SP
GET /LSC/WebHome HTTP/1.1
Host: wiki.ligo.org
HTTP/1.1 302 Found
Location: https://login.ligo.org/idp/...
GET https://login.ligo.org/idp/...
HTTP/1.1 404 Authorization Required
GET https://login.ligo.org/idp/...
Authorization: Basic xx7kdfaow
HTTP/1.1 302 Found
Location: https://wiki.ligo.org/...
GET /Shibboleth.sso/...
Host: wiki.ligo.org
HTTP/1.1 302 Found
Location: https://wiki.ligo.org/LSC/...
Set-Cookie: _shibsession_6yw72j...
GET /LSC/WebHome HTTP/1.1
Host: wiki.ligo.org

IdP

IdP authenticates the user and sends back to SP.
IdP asserts that the user has authenticated.

- Often includes some details about how.
- Often includes some details about when.
- Usually asserts an identifier for the user.
  - may be *opaque* and/or *targeted*.
- Sometimes asserts attributes about user.

Details depend on format chosen by IdP and SP.

Web AuthN/Z Protocols

OpenID:

- Relatively simple.
- Supported by Google, FB, Twitter, Yahoo, ...
- Good adoption in web 2.0 spaces.
- Not focused on preserving privacy.
- Not focused on rich attribute exchange.
  - OpenID Authentication 2.0 and OpenID Attribute Exchange 1.0 helped improve that.

Web AuthN/Z Protocols

OAuth:

- Focused on authorization, not authentication.
- Type of limited delegation.
- Allow site A (Facebook) to access site B (Instagram) on your behalf.

Web AuthN/Z Protocols

OpenID Connect:

- Next generation OpenID.
- Builds on top of and incorporates OAuth 2.
- More complex but delivers more functionality.
- Tension between enterprise needs and “simple”.
- Slow uptake at this moment...

Web AuthN/Z Protocols

SAML:

- More complex than OpenID.
- Strong privacy preserving.
- Strong attribute exchange.
- Good adoption in higher education.
- Limited adoption outside of higher education.
  - More uptake in research space recently.

LIGO Chose SAML

- Strong support from higher education.
  - Strong support from Internet2.
  - Strong support from InCommon.
- Rich attribute assertion mechanisms
  - Less concerned with privacy preservation.
- Straightforward path away if necessary:
  - “Social2SAML” gateways.
  - Allow slow transition if necessary.

LIGO SAML & Shibboleth

LIGO has significant investment in Shibboleth.

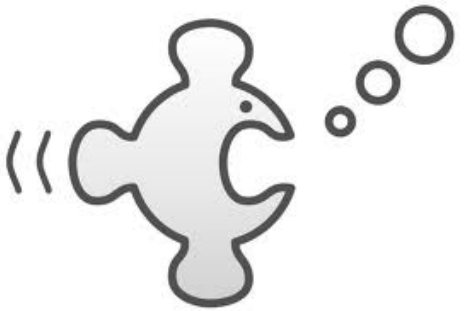
- IdP is Shibboleth 2.3.x.
- Over 60 Shibboleth SPs now.
- Member of the Shibboleth consortium.
- Currently 5+ staff with Shibboleth training.

Shibboleth.

Shibboleth is an implementation of SAML.

- Originally started by Internet2 in US.
- Now funded by its own consortium.
  - Support both in Europe and US.
- Provides:
  - Identity Provider (Java servlet).
  - Service Provider (Native C Apache module).
  - Centralized or Embedded Discovery Service.

SAML Tools



- SimpleSAMLphp.
  - open source.
  - both IdP and SP functionality.
  - primarily a European project.
- OpenAM
  - IdP.
  - evolution of OpenSSO from Sun/Oracle.
  - open source with support from ForgeRock.
- Ping Identity
  - private company.
  - IdP.

IAM Components

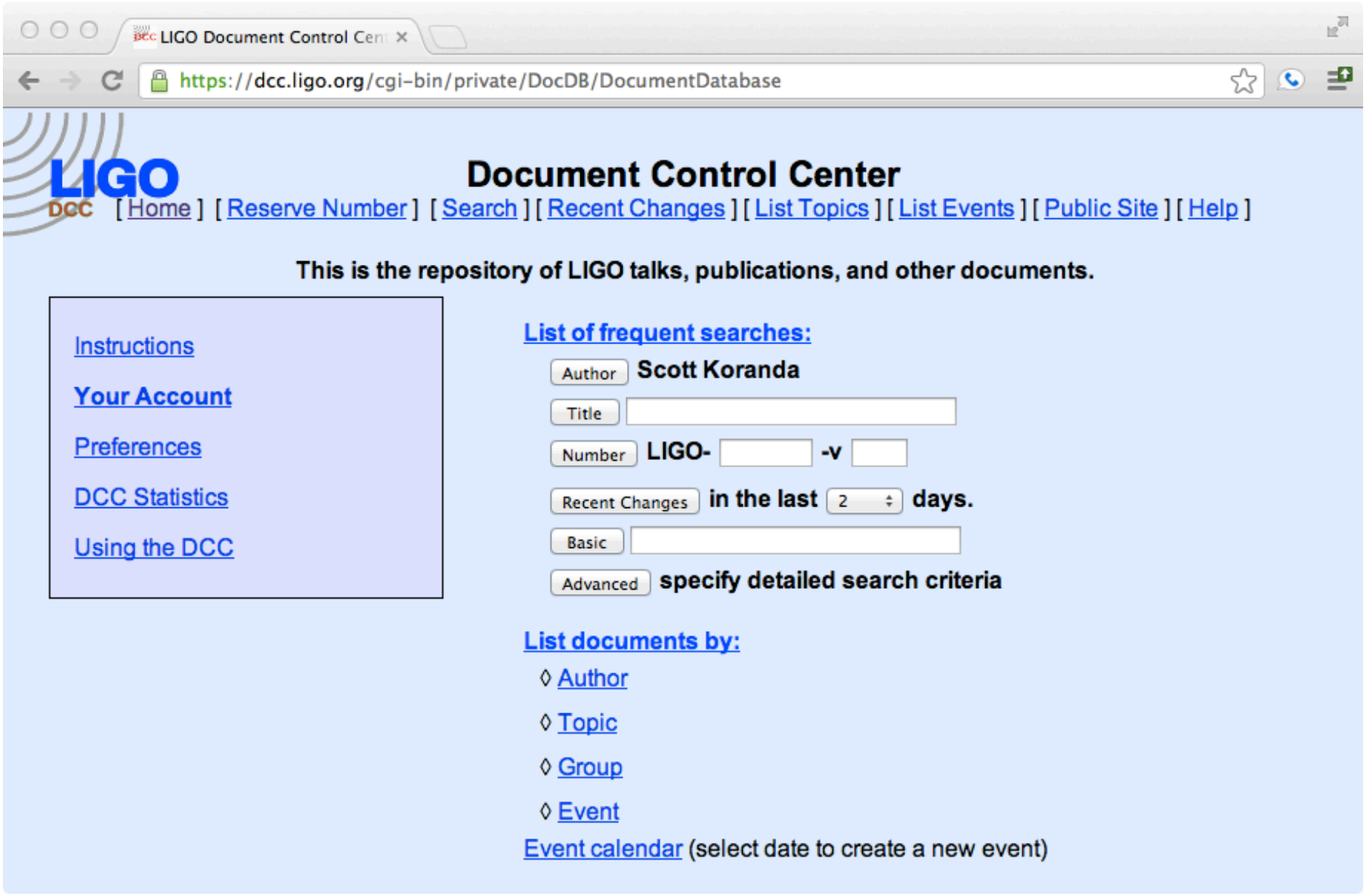
- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

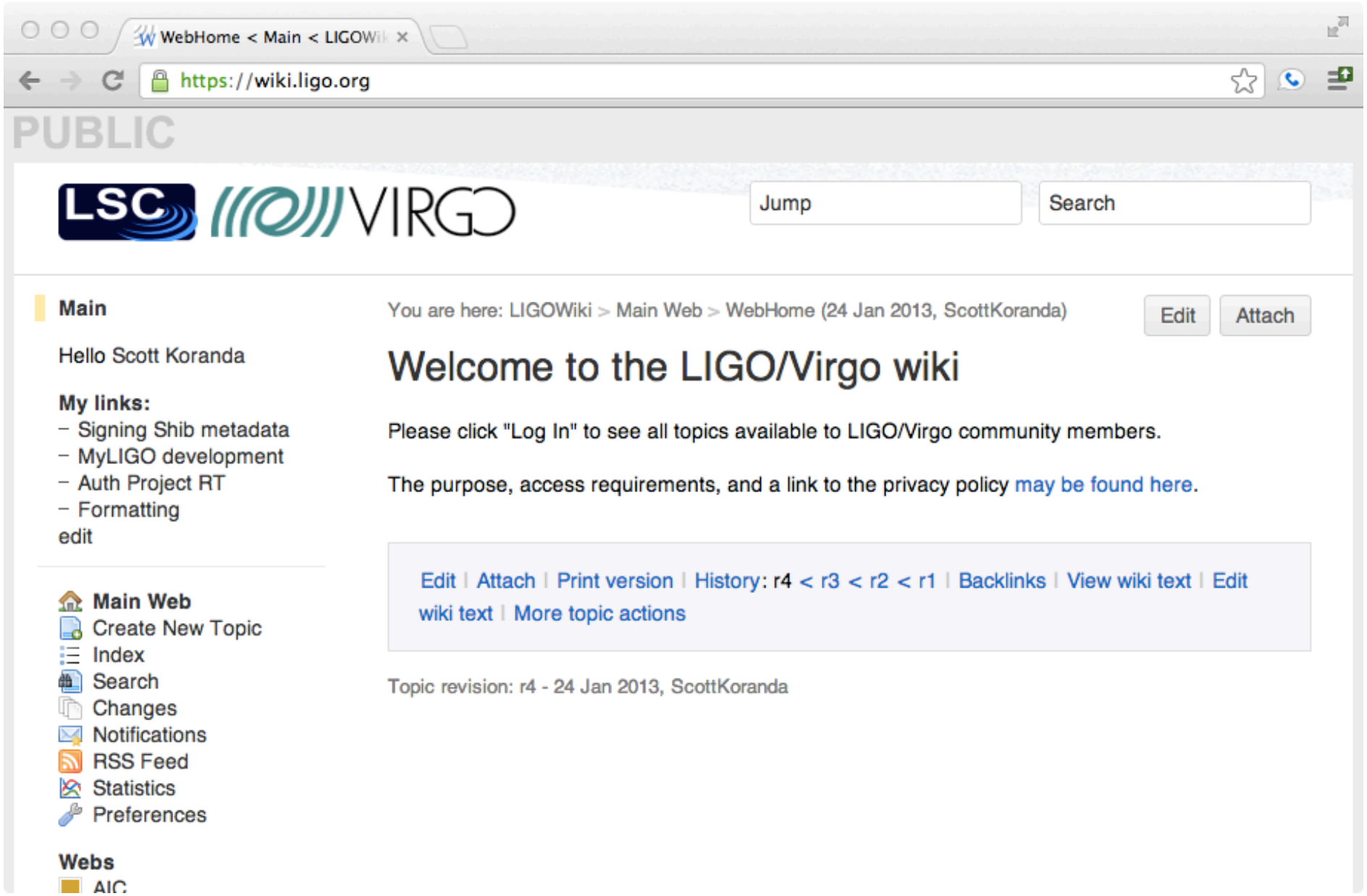
IAM Component: Service Provider

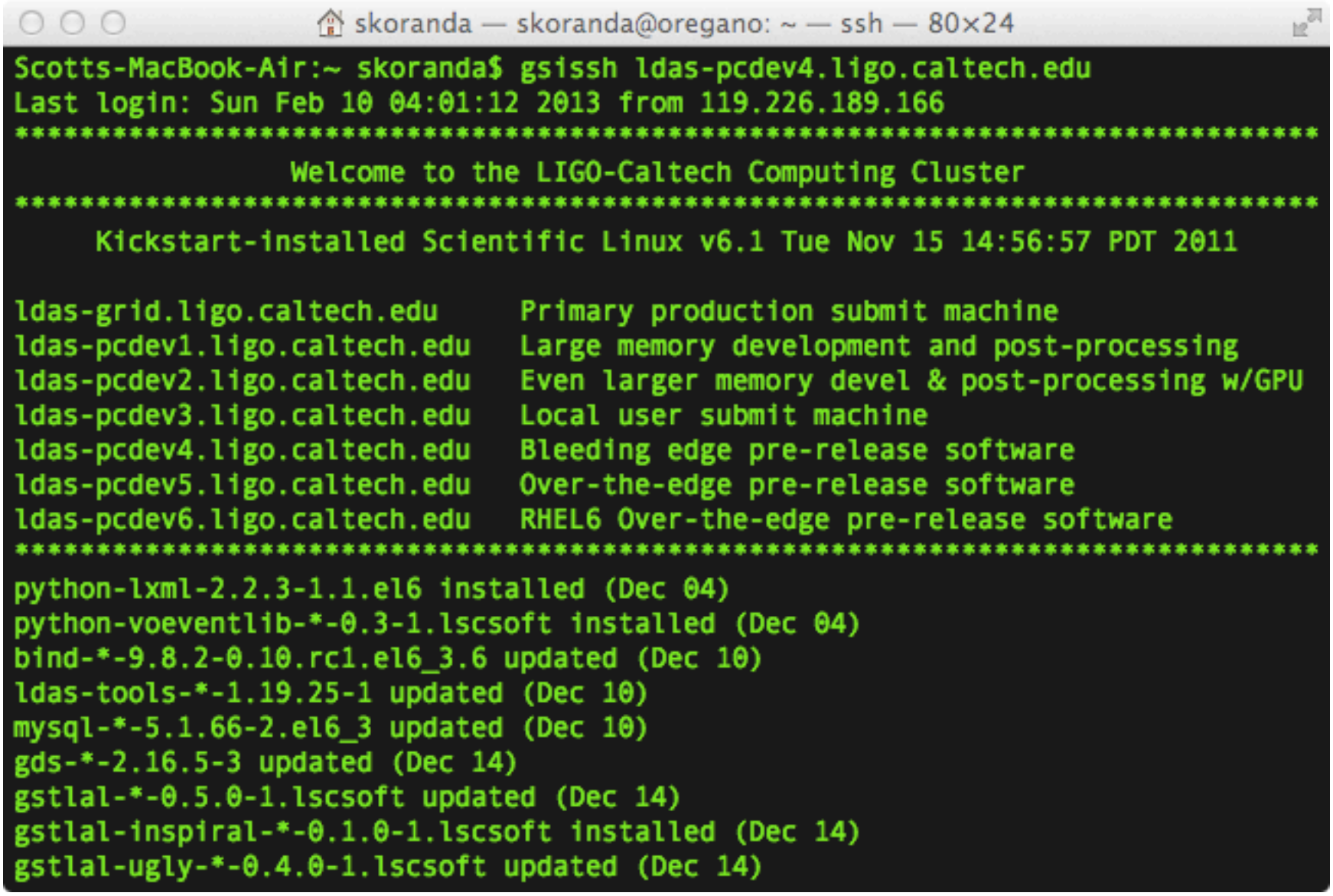
Term “service provider” (SP) most often used in web context.

Any service or tool (resource) users or their delegates access.

Access to the SP usually requires authentication *and* authorization.


LIGO Document Control Cen
https://dcc.ligo.org/cgi-bin/private/DocDB/DocumentDatabase
LIGO
DCC
Document Control Center
[Home] [Reserve Number] [Search] [Recent Changes] [List Topics] [List Events] [Public Site] [Help]
This is the repository of LIGO talks, publications, and other documents.
Instructions
Your Account
Preferences
DCC Statistics
Using the DCC
List of frequent searches:
Author
Scott Koranda
Title
Number
LIGO-
-v
Recent Changes
in the last
2
days.
Basic
Advanced
specify detailed search criteria
List documents by:
◊ Author
◊ Topic
◊ Group
◊ Event
Event calendar (select date to create a new event)


WebHome < Main < LIGOWi
https://wiki.ligo.org
PUBLIC
LSC
VIRGO
Jump
Search
Main
Hello Scott Koranda
My links:
– Signing Shib metadata
– MyLIGO development
– Auth Project RT
– Formatting
edit
Main Web
Create New Topic
Index
Search
Changes
Notifications
RSS Feed
Statistics
Preferences
Webs
AIC
You are here: LIGOWiki > Main Web > WebHome (24 Jan 2013, ScottKoranda)
Edit
Attach
Welcome to the LIGO/Virgo wiki
Please click "Log In" to see all topics available to LIGO/Virgo community members.
The purpose, access requirements, and a link to the privacy policy may be found here.
Edit | Attach | Print version | History: r4 < r3 < r2 < r1 | Backlinks | View wiki text | Edit wiki text | More topic actions
Topic revision: r4 - 24 Jan 2013, ScottKoranda


skoranda — skoranda@oregano: ~ — ssh — 80×24
Scotts-MacBook-Air:~ skoranda$ gsissh ldas-pcdev4.ligo.caltech.edu
Last login: Sun Feb 10 04:01:12 2013 from 119.226.189.166
****
Welcome to the LIGO-Caltech Computing Cluster
****
Kickstart-installed Scientific Linux v6.1 Tue Nov 15 14:56:57 PDT 2011
ldas-grid.ligo.caltech.edu Primary production submit machine
ldas-pcdev1.ligo.caltech.edu Large memory development and post-processing
ldas-pcdev2.ligo.caltech.edu Even larger memory devel & post-processing w/GPU
ldas-pcdev3.ligo.caltech.edu Local user submit machine
ldas-pcdev4.ligo.caltech.edu Bleeding edge pre-release software
ldas-pcdev5.ligo.caltech.edu Over-the-edge pre-release software
ldas-pcdev6.ligo.caltech.edu RHEL6 Over-the-edge pre-release software
****
python-lxml-2.2.3-1.1.el6 installed (Dec 04)
python-voeventlib-*-0.3-1.lscsoft installed (Dec 04)
bind-*-9.8.2-0.10.rc1.el6_3.6 updated (Dec 10)
ldas-tools-*-1.19.25-1 updated (Dec 10)
mysql-*-5.1.66-2.el6_3 updated (Dec 10)
gds-*-2.16.5-3 updated (Dec 14)
gstlal-*-0.5.0-1.lscsoft updated (Dec 14)
gstlal-inspiral-*-0.1.0-1.lscsoft installed (Dec 14)
gstlal-ugly-*-0.4.0-1.lscsoft updated (Dec 14)

IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: Groups, Roles, Privileges Manager

Access management often maps to **groups**.

"Only members of the 'executive committee group' may read and edit the ExComm web at wiki.ligo.org"

```
Set ALLOWWEBVIEW =
Communities:LVC:LSC:ExecComm:ExecCommGroupMembers
```

Groups, Roles, Privileges Manager

Access management also often maps to **roles**.

- Role-Based Access Control (RBAC).

“The Director of LIGO and the LIGO Scientific Collaboration Spokesperson may download this document from the document control center (DCC).”

Groups, Roles, Privileges Manager

Many tools include their own groups, roles, and privileges management capabilities.

- Often these offer only limited functionality.
- Not possible to share across organization.

Centralized (specialized) tools for group, role, privilege management:

- LDAP (and tools built on top of it)
- VOMS
- Grouper

Groups, Roles, Privileges Manager

What to look for in centralized groups/roles/privileges tool:

- Set math.
  - compose, complement.
- No imposed hierarchy.
  - Should not assume a tree hierarchy.
  - No assumptions about organizational structure.
- Time management.
  - Effective dates and times.
  - Auditing (point-in-time).
- Manage entities and objects—not just people.

Grouper

- Internet2 in the United States.
- Support for set math.
  - both composition and complement.
- No imposed structure.
- Reflection (provisioning) into LDAP.
- Manage groups, roles, and privileges.
  - RBAC support.

Grouper

- Support for time management:
  - Effective dates/times.
  - Point-in-time auditing.
- Strong support for delegation.
  - Let group leaders manage their own memberships.
- Java servlet with relational database backend.
- Significant learning curve.


LIGO groups manager
https://grouper.ligo.org/grouper/browseStemsAll.do?currentNode=4f9bc5bc-...
LIGO
LSC
Welcome Scott Koranda
Act as admin
Change
My tools
Explore
Search
Folder workspace
Group workspace
Entity workspace
Group types
Help
LIGO
Roster
LIGO group management based on Grouper from
EXPLORE
Browse groups hierarchy
You can look for groups throughout the hierarchy.
(You might not be able to see some groups if you lack appropriate privileges.)
Browse or list groups
Current location is:
Root: Communities: LVC: LIGOLab
Showing 1-11 of 11 items
CIT
DCC
External
Instrumental
LHO
LLO
MIT
Safety
DirectorGroupMembers
LIGOLabGroupManagers
LIGOLabGroupMembers

IAM Components

- User registry
- Directory
- Authentication store
- Identity provider
- Service provider
- Group, role, and privilege manager
- Attribute authority

IAM Component: Attribute Authority

Attribute Authority (AA) asserts attributes and attribute values.

```
scott.koranda@ligo.org:
   givenName: Scott
   sn: Koranda
   eduPersonAffiliation: member
   isMemberOf: LIGO
```

Attribute Authority

Most often attributes of people.

- But could be attributes about other entities.

Question of which source is authoritative for which attributes is an open research question.

Attribute Authority

Question of which source is authoritative for which attributes is an open research question:

- LIGO AA asserts scott.koranda@ligo.org is a member of LIGO group
- KAGRA AA asserts yoichi.aso@kagra.org is a member of KAGRA group
- Who asserts scott.koranda@ligo.org and yoichi.aso@kagra.org are members in the joint LIGO-KAGRA working group?

Attribute Authority

Common AA stores or services:

- LDAP
  - Easy integration with spectrum of clients.
  - Solid open source implementations.
- Shibboleth IdP
  - Attribute assertion with authentication event.
  - Attribute assertion without authentication event.
    - Standalone AA functionality.

PART IV – *Federated Identity*

"I am Pavel Chekov, a commander in Starfleet. United Federation of Planets Service Number 656-5827D."

Star Trek IV: The Journey Home

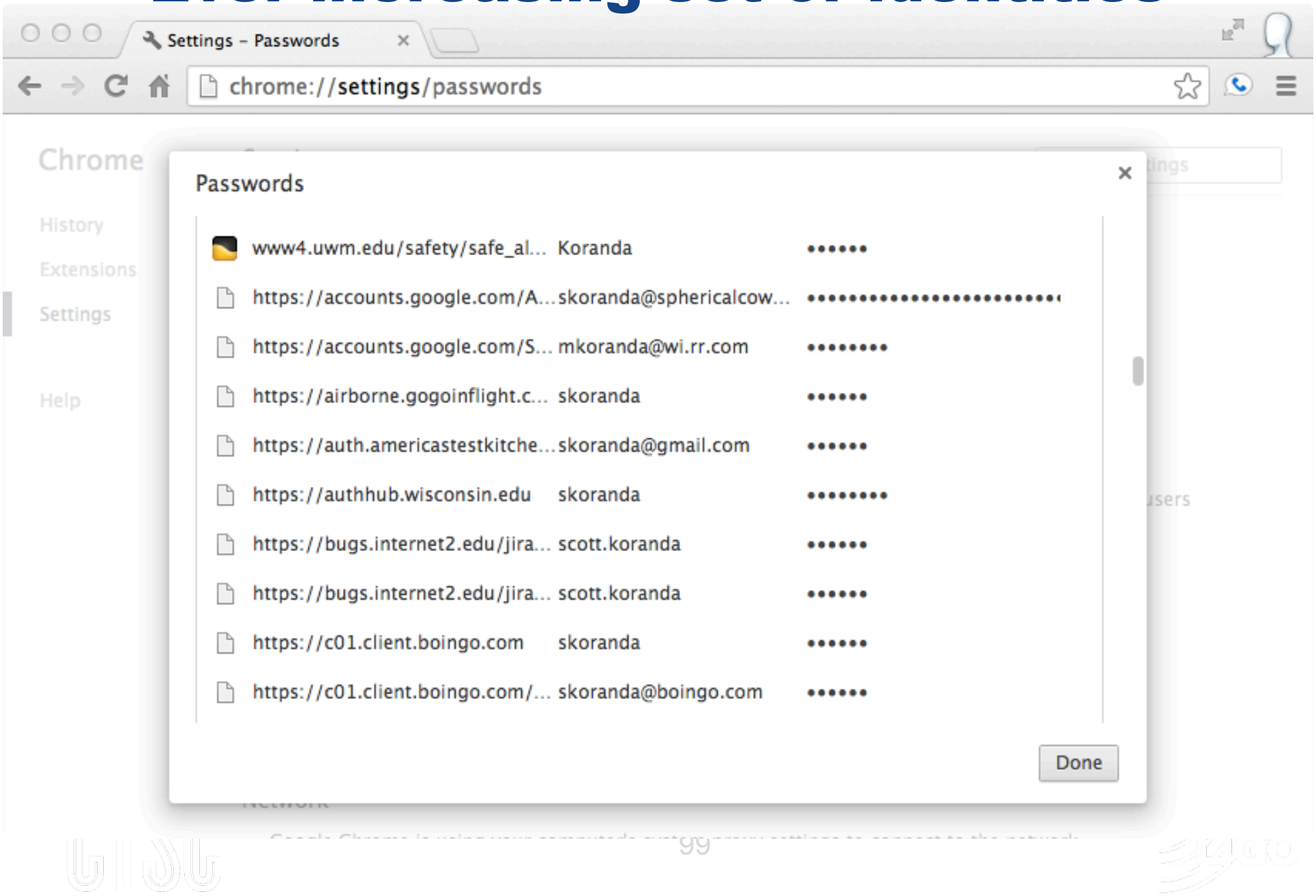
Federated Versus “Local” Identity

“Local” identity is the identity provisioned for you within a single identity or security domain.

Often the identity provisioned for you by some existing application, service, or tool.

Want to access (login) our project’s resources? Create (yet another!) account.

Ever increasing set of identities



Federated Identity

Federated identity is an identity you can use across multiple security or identity domains.

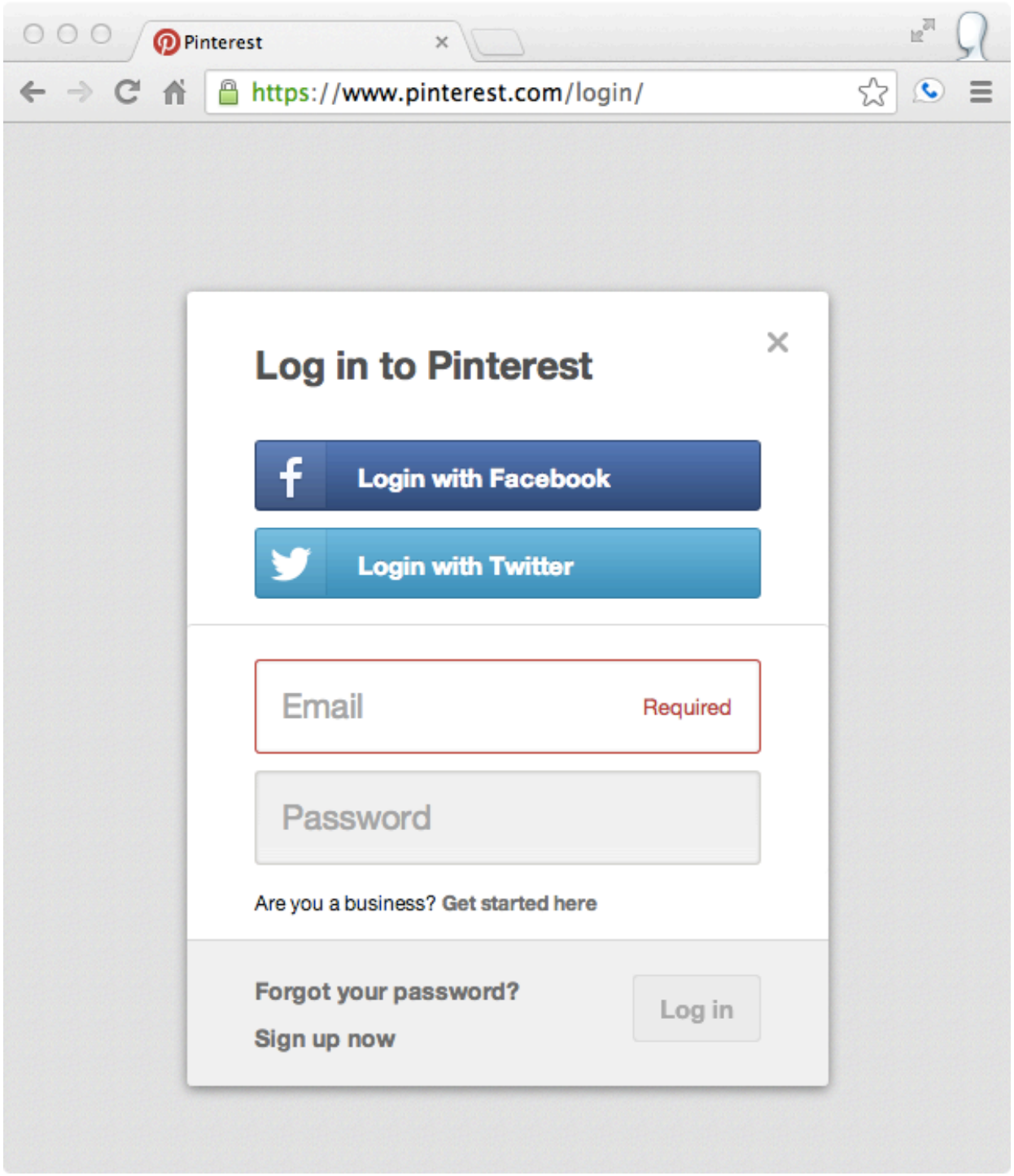
Related to, but not the same as, single sign-on (SSO).

SSO provides authentication within a single identity domain (fuzzier for VOs).

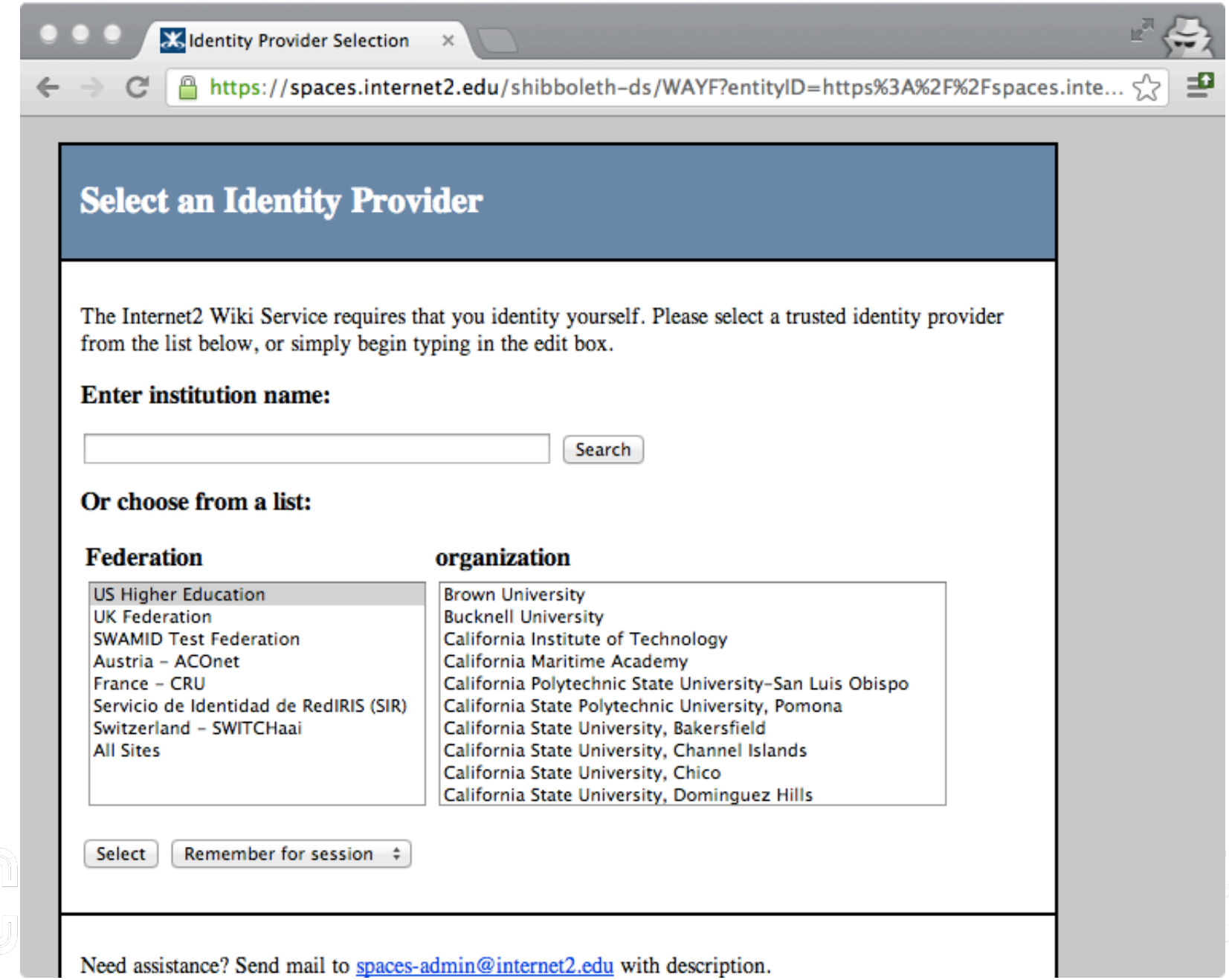
Federated Identity

Might have see already with newer web 2.0 apps.

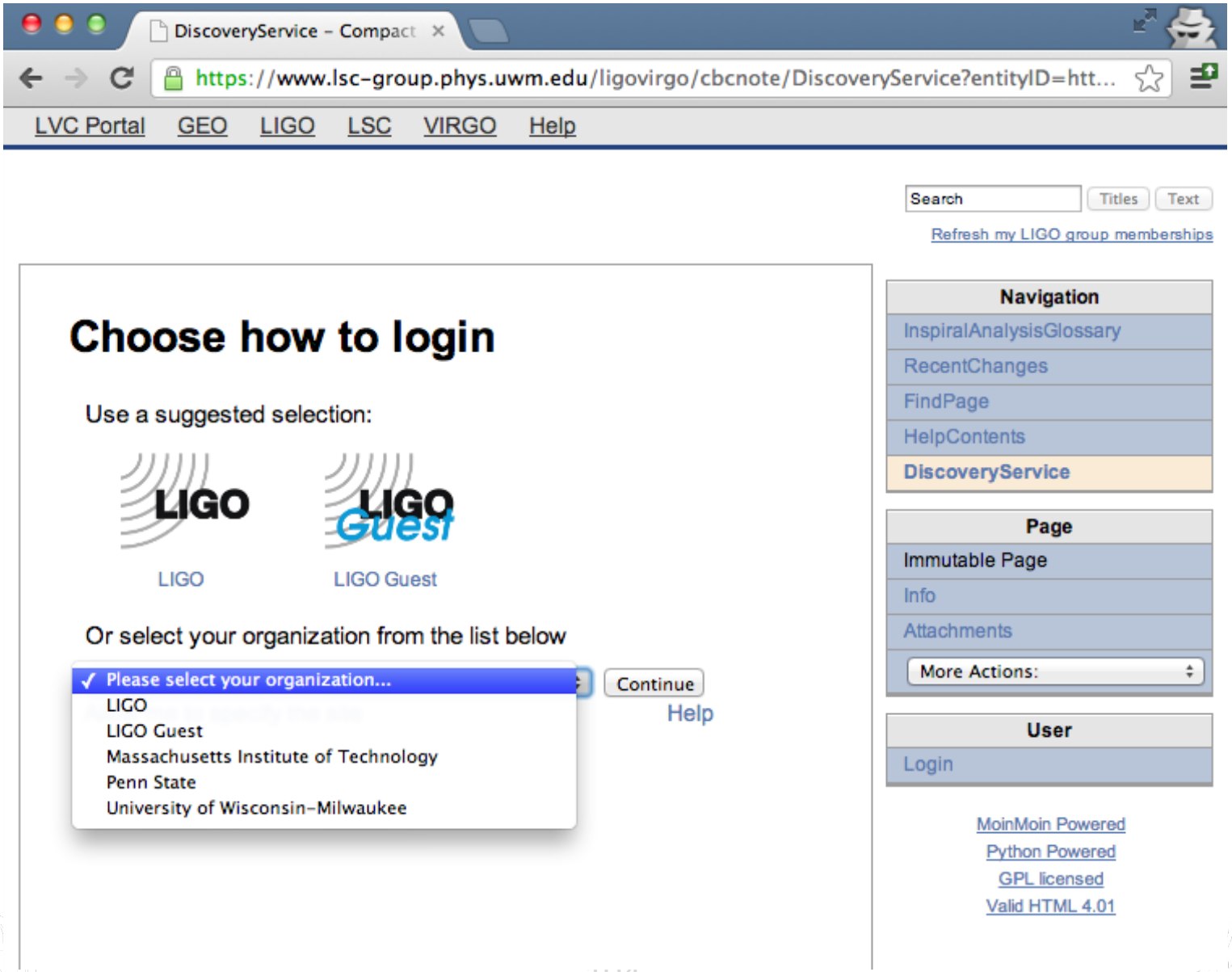
“Login with your Google/Facebook/Twitter account”


Pinterest
https://www.pinterest.com/login/
Log in to Pinterest
Login with Facebook
Login with Twitter
Email
Required
Password
Are you a business? Get started here
Forgot your password?
Sign up now
Log in

Higher Ed & Research Identities



LIGO Leverages Federated Identity



Federated Identity

Pros:

- Users do not have to create new account.
  - “Yet another new account”
- Faster for users to access resource.
- Easier for users to access resource.
- Single credential often protected better.
  - Only one account to manage so manage it well!

Federated Identity

Cons:

- New experience for users.
- More mouse clicks just to login to service.
- More complexity for service and infrastructure.
- Error handling more difficult to provide.
- Single credential when compromised is disaster.
  - Bad actors have access across multiple security domains instead of just one.

Federated Identity: LIGO Use Cases

Consume federated identity and get out of business of providing identity.

- Save substantial help desk support effort.
- Save substantial infrastructure support effort.

Goal, but will be long time coming.

- Need excellent command line support.
- Need sufficient levels of assurance from remote IdPs.
- Need to access identities from around the world.

Federated Identity: LIGO Use Cases

Streamline collaboration with partners.

- KAGRA (Japan)
- Virgo (French/Italian)
- LIGO-India

Prevent members in each collaboration from having to request and manage identities and credentials provisioned by other collaborations.

Federated Identity: LIGO Use Cases

Streamline collaboration with astronomers, astrophysicists, and other scientists.

Share, when appropriate, access to analysis results, data, and other scientific work product with colleagues.

Federated Identity: LIGO Use Cases

Ease processes for review committees, funding agency representatives, and other VIPs.

Prevent VIPs from having to create a LIGO identity or account just to participate on a review panel.

Trust and Federated Identity

“All the world is made of faith, and trust, and pixie dust.”

J. M. Barrie, Peter Pan

Trust and Federated Identity

How do I know I can trust a remote IdP?

How does the remote IdP know it can trust the SP?

- Doesn't want to allow any service to use it for authenticating users.

Substantially harder when IdP and SP not part of the same organization or security domain.

Trust the Hard Way

Each IdP, SP negotiates trust in a point-to-point model:

- What identifier is exchanged?
- How information is encrypted and signed?
- Which attributes are asserted?
- How attributes are asserted?
- How attributes are consumed?
- Which privacy policies are in effect?

Legal and policy ramifications cannot be ignored, even for science projects.

Need Scalable Trust Model

Framework for IdPs and SPs to agree to common policies and operating procedures in order to bootstrap trust efficiently across the participants.

IdPs and SPs using SAML as web Authz framework rely on SAML Identity Federations.

SAML Identity Federation

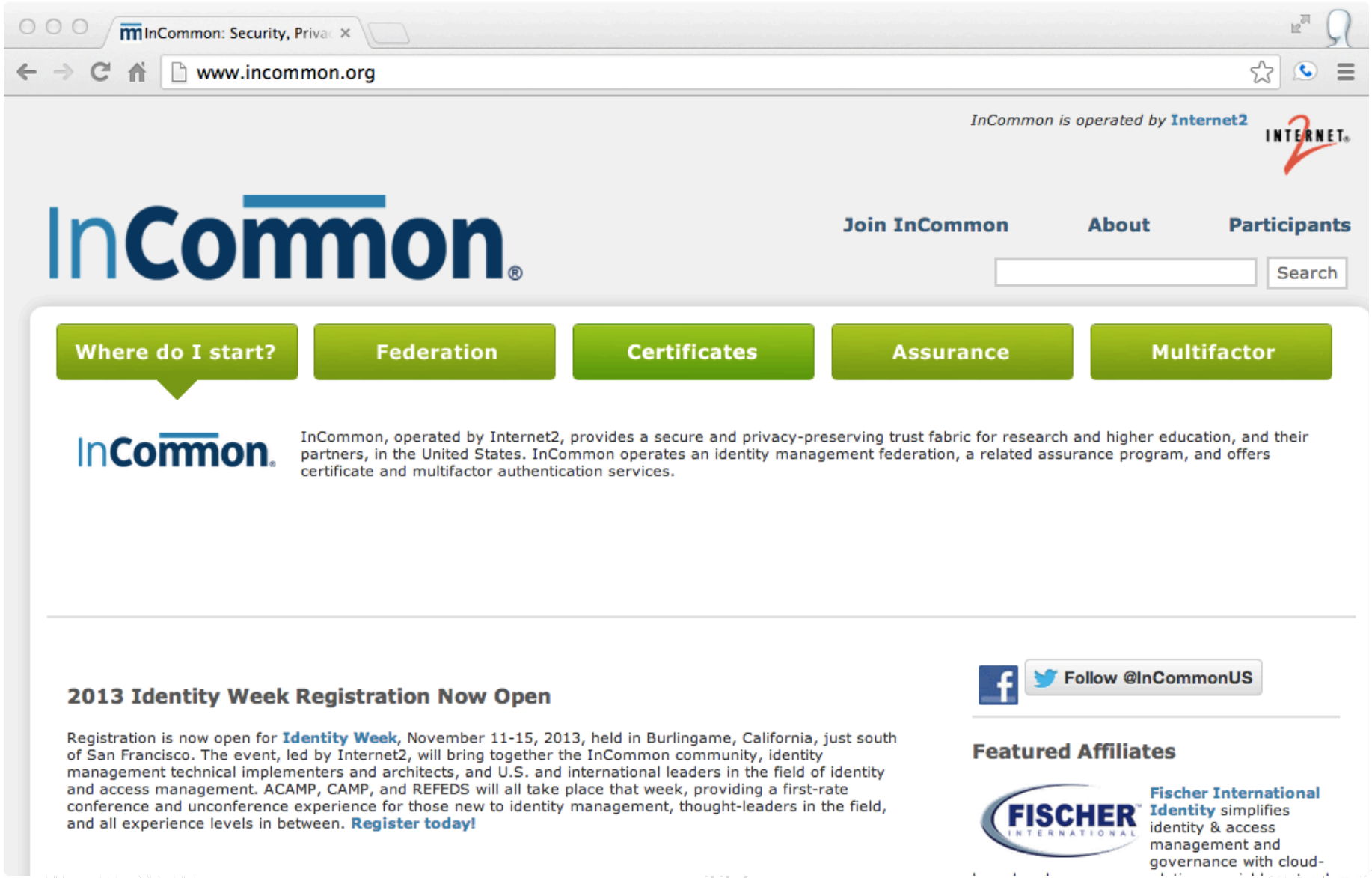
IdP and SP participants agree on:

- Policies for operating IdPs and SPs.
- Establishing trust through exchange of SAML metadata.
  - Details about each IdP and SP, their service endpoints, and how assertions will be signed and encrypted.
- Policies for how metadata is managed.

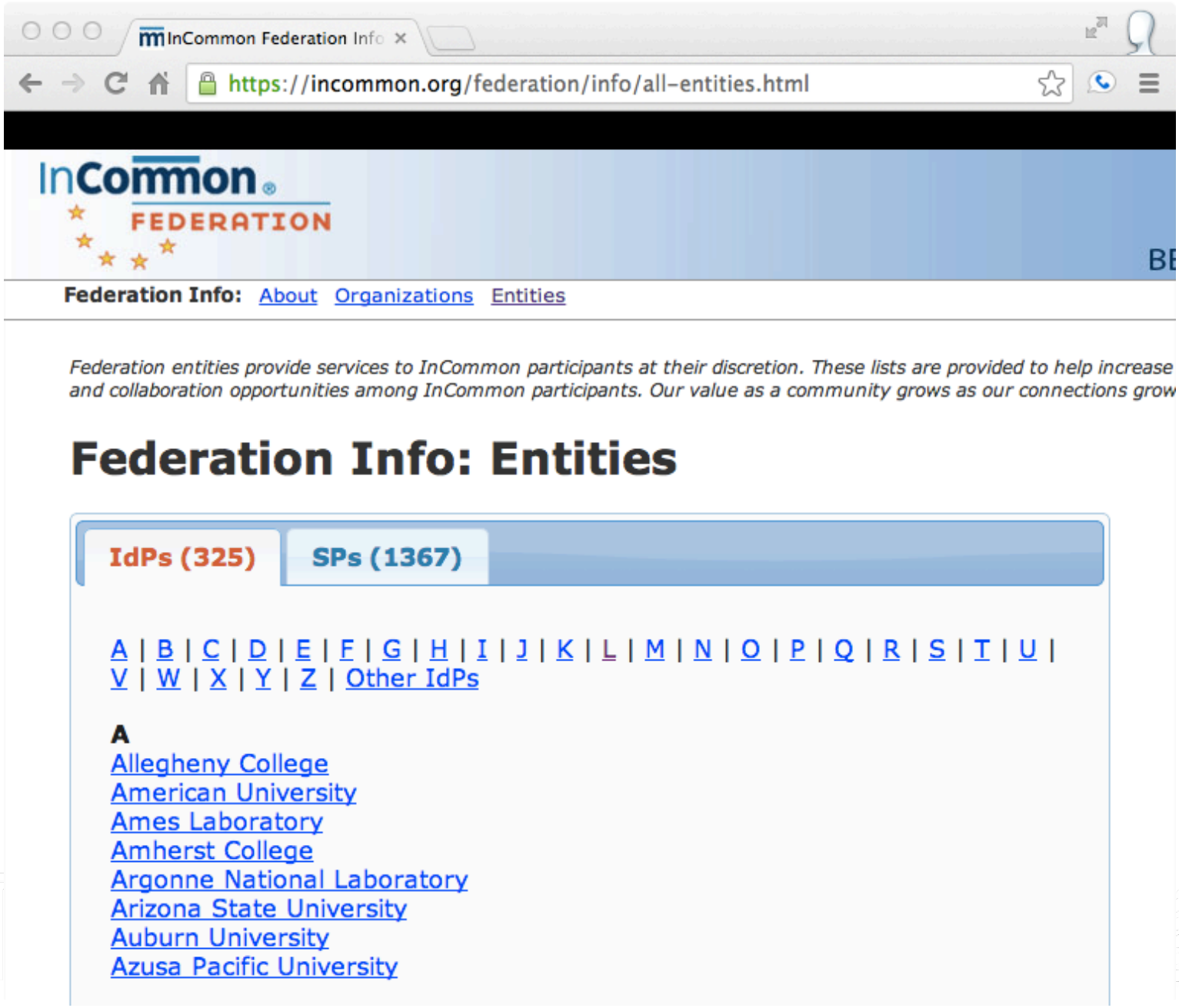
SAML Identity Federations

Most SAML identity federations established and operated by national research and education network (NREN) providers.

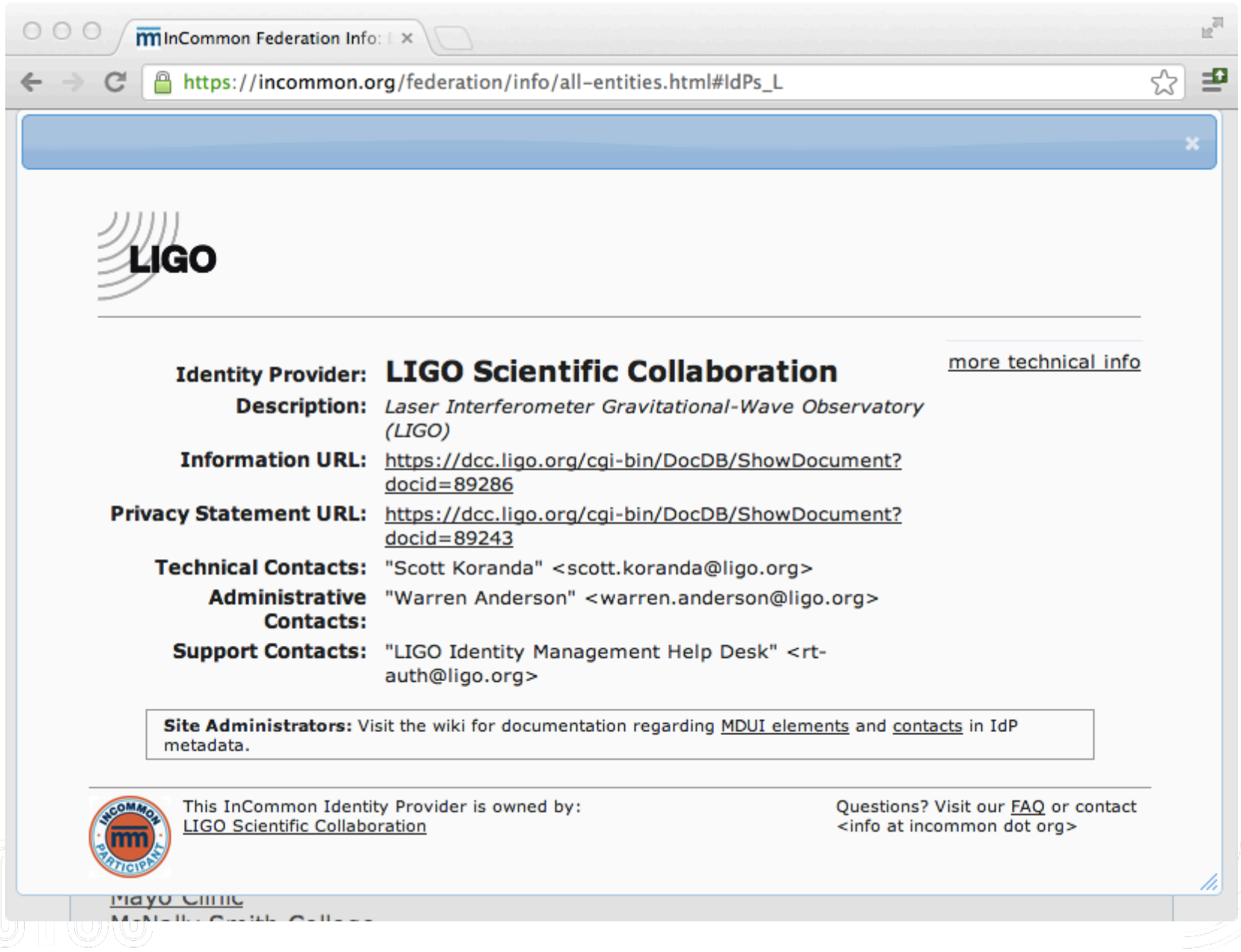
US SAML Identity Federation



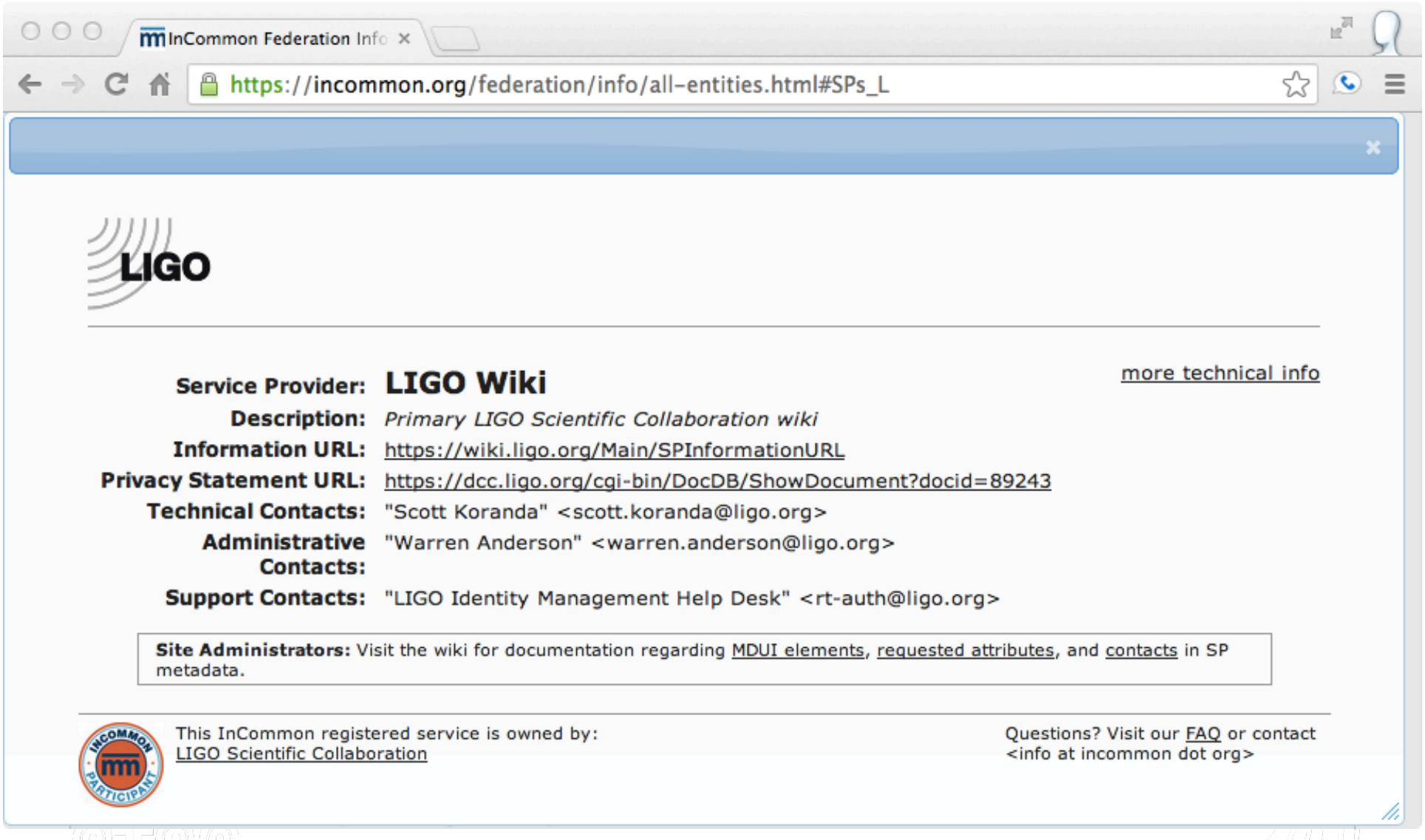
325 IPs and 1367 SPs



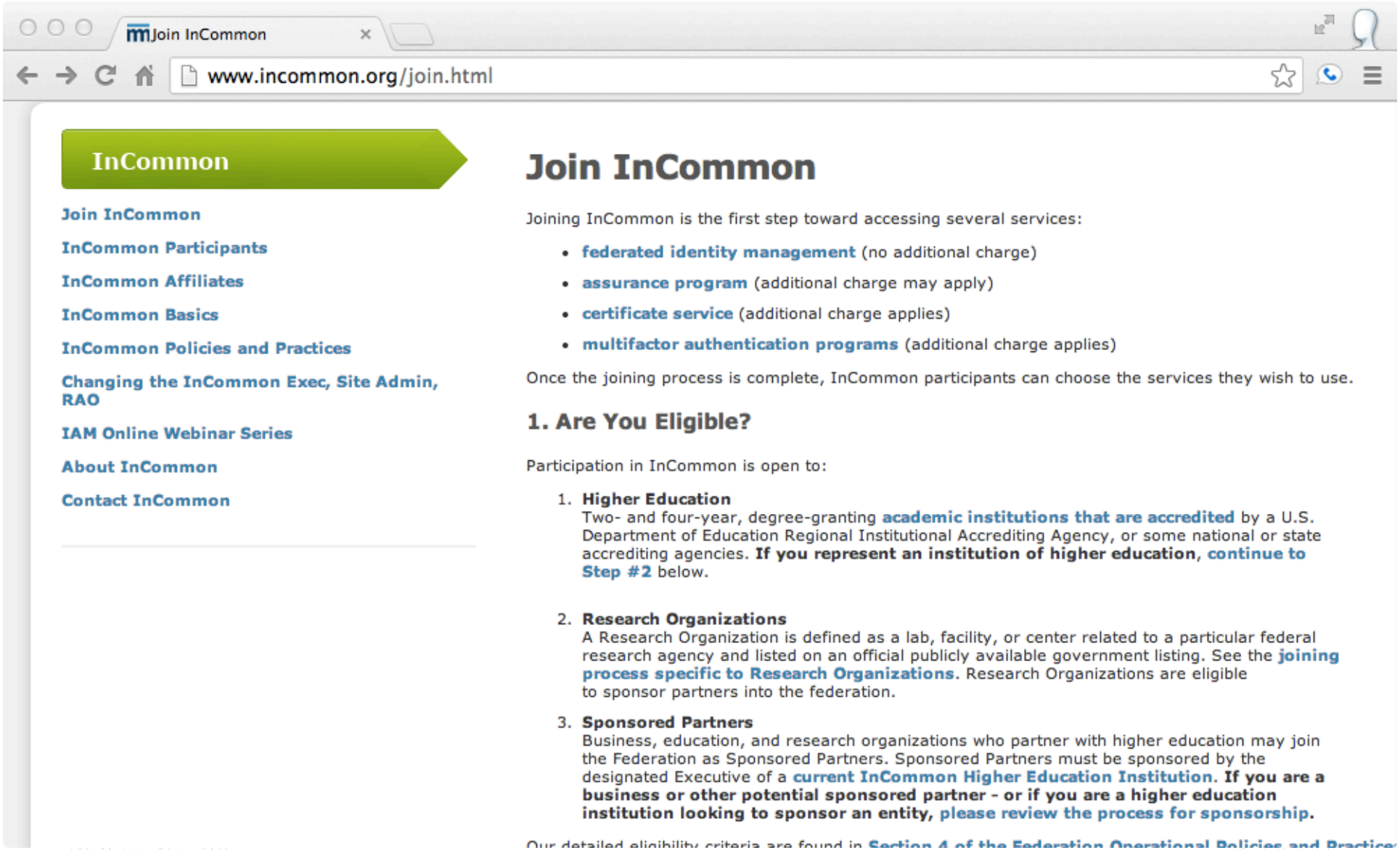
LIGO IdP in InCommon



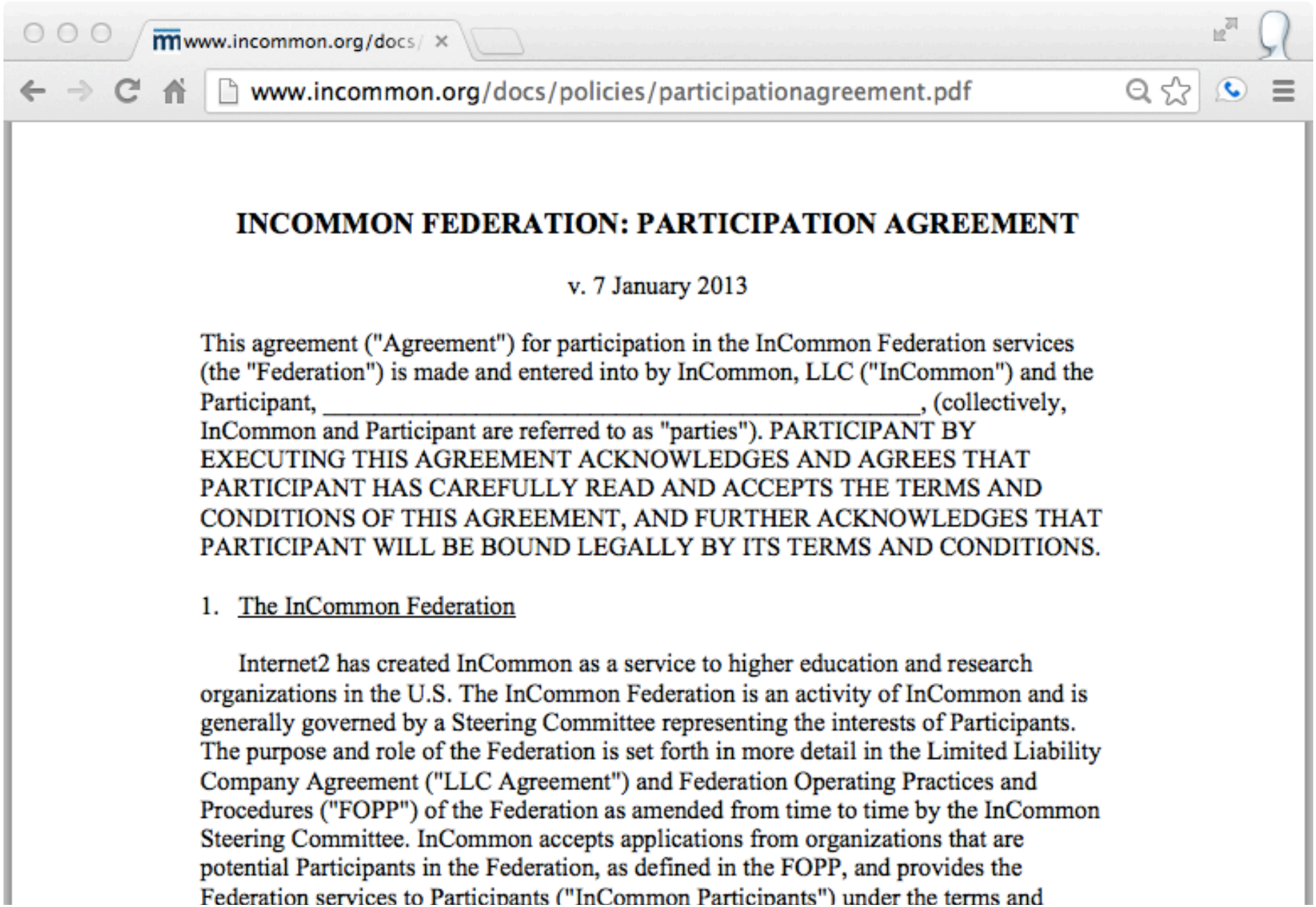
LIGO SP in InCommon



Research VOs May Join



VOs Sign Participant Agreement



VOs pay $ to InCommon

Challenges Joining InCommon

Many VOs not legal entities.

- LIGO is not a legal entity.
- Caltech signed on behalf of LIGO.
  - Includes people not on Caltech campus.
  - Why should Caltech assume that risk?
- InCommon needs to broaden interpretation of sharing risk.
  - Indemnification and insurance not only way to mitigate risk.
  - Need better models for distributed research VOs.
- VOs should leverage willing campus sponsors.

Challenges Joining InCommon

Culture based on campuses and not VOs.

- Changing but still an issue at times.
- Different balance between risk and rewards.
- Different timescale than many VOs.
  - 3 years for major initiative not uncommon.
  - A research VO may come and go in 3 years.
  - Positive is long term stability.

Joining InCommon

Joining InCommon is a legal agreement.

Does not require technical infrastructure so can begin joining process early before ready for consuming federated identity.

Leveraging InCommon

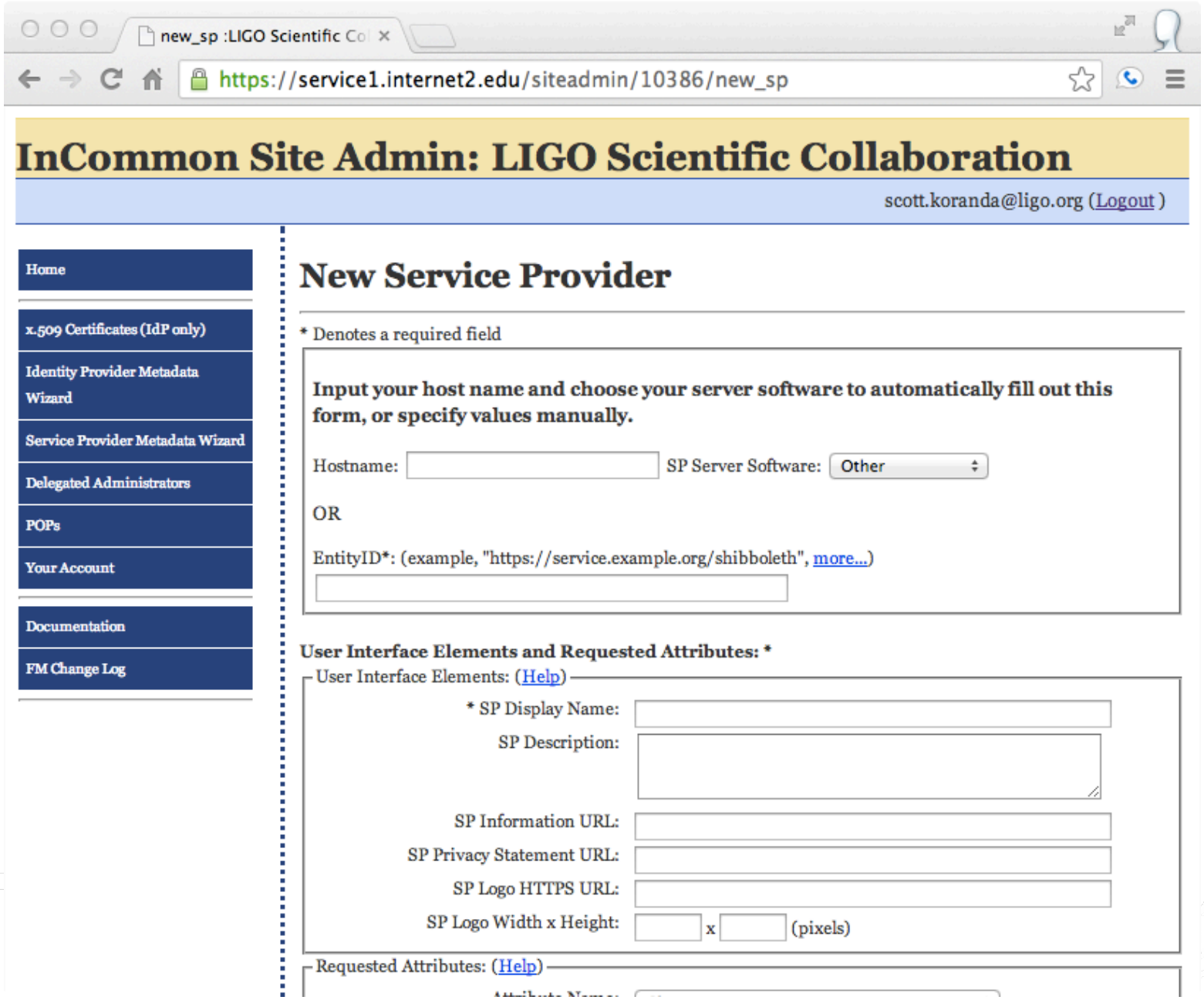
Register SP to consume federated identities.

- Publish SP metadata into InCommon feed.
- Feed consumed by InCommon IdPs.
- Enables interoperability between SP and IdPs.

Step 0: deploy Shibboleth SP

- Use your best web application people.

Publish SP into InCommon



Publish SP in InCommon

Sounds great!

- Deploy Shibboleth on your web server.
- Publish SP into InCommon metadata.
- Consume federated identities from 300+ IdPs.
- Never issue a password again!

What's the catch?

Publishing SP Enables Interoperability

Does **NOT** guarantee interoperability.

- IdPs free to ignore your SP and some will.
  - A few “well known” campuses do not collaborate by default.
- Does your application need anything more than authentication?
  - Default for many IdPs is binary yes/no of authentication event.

InCommon IdPs

Most IdPs send opaque, targeted, transient identifier and nothing else.

<saml2:NameID
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient”
NameQualifier="https://login.ligo.org/idp/shibboleth”
SPNameQualifier="https://wiki.ligo.org/shibboleth-sp”
>_708b4a90108f5cb2a424534495ffd081</saml2:NameID>

Driven by privacy concerns (FERPA anyone?)

Yes, given name, sn, email considered private.

InCommon IdPs

“Who are you?"
"No one of consequence."
"I must know."
"Get used to disappointment.”

William Goldman, The Princess Bride

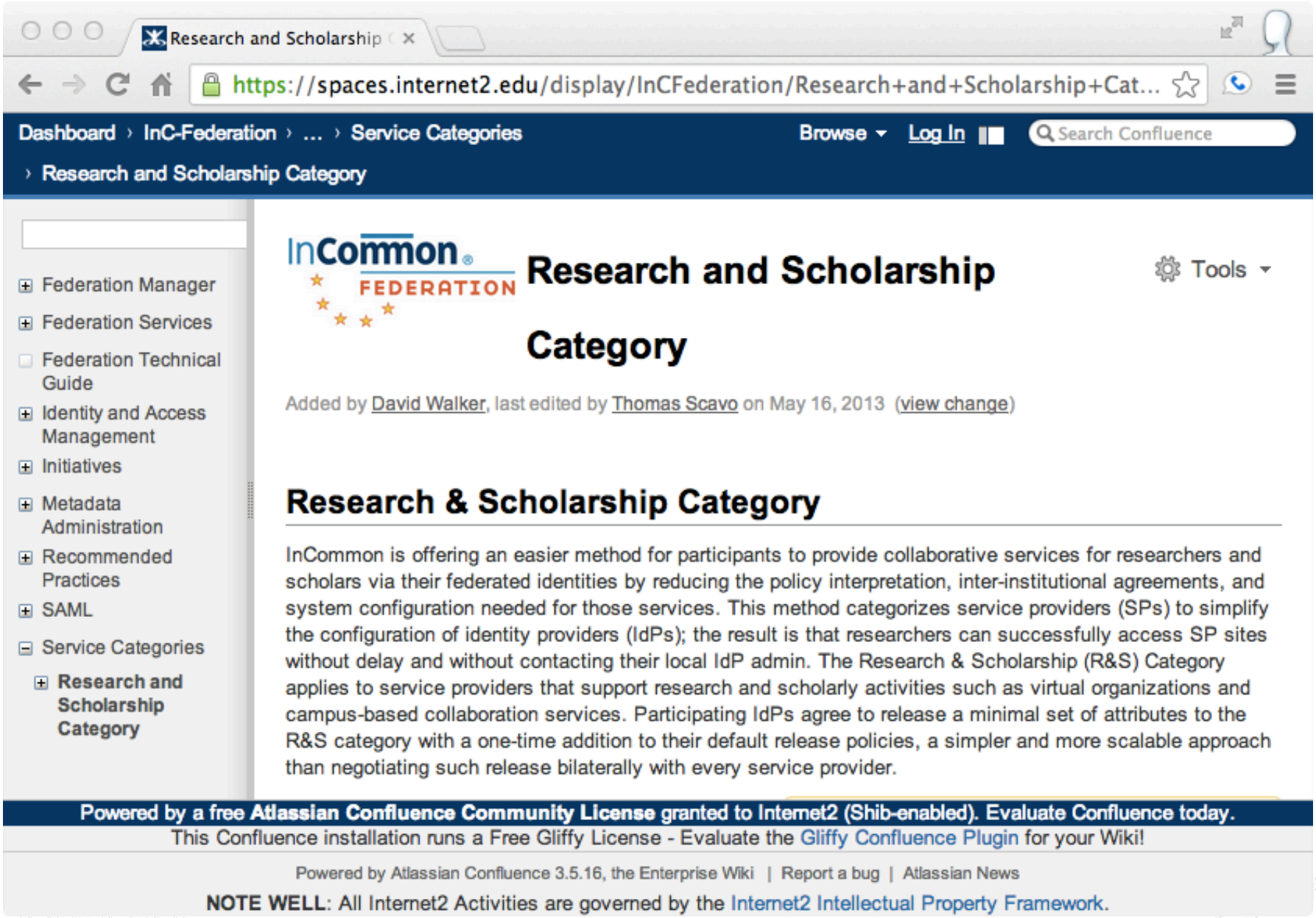
Applications Need More Attributes

Most VO web applications require more from a federated identity:

- given name
- family name
- email
- non-transient or persistent
- non-targeted or same for all SPs
- non-opaque since often “seen” by humans

This default for most InCommon IdPs is a serious limitation for science VOs.

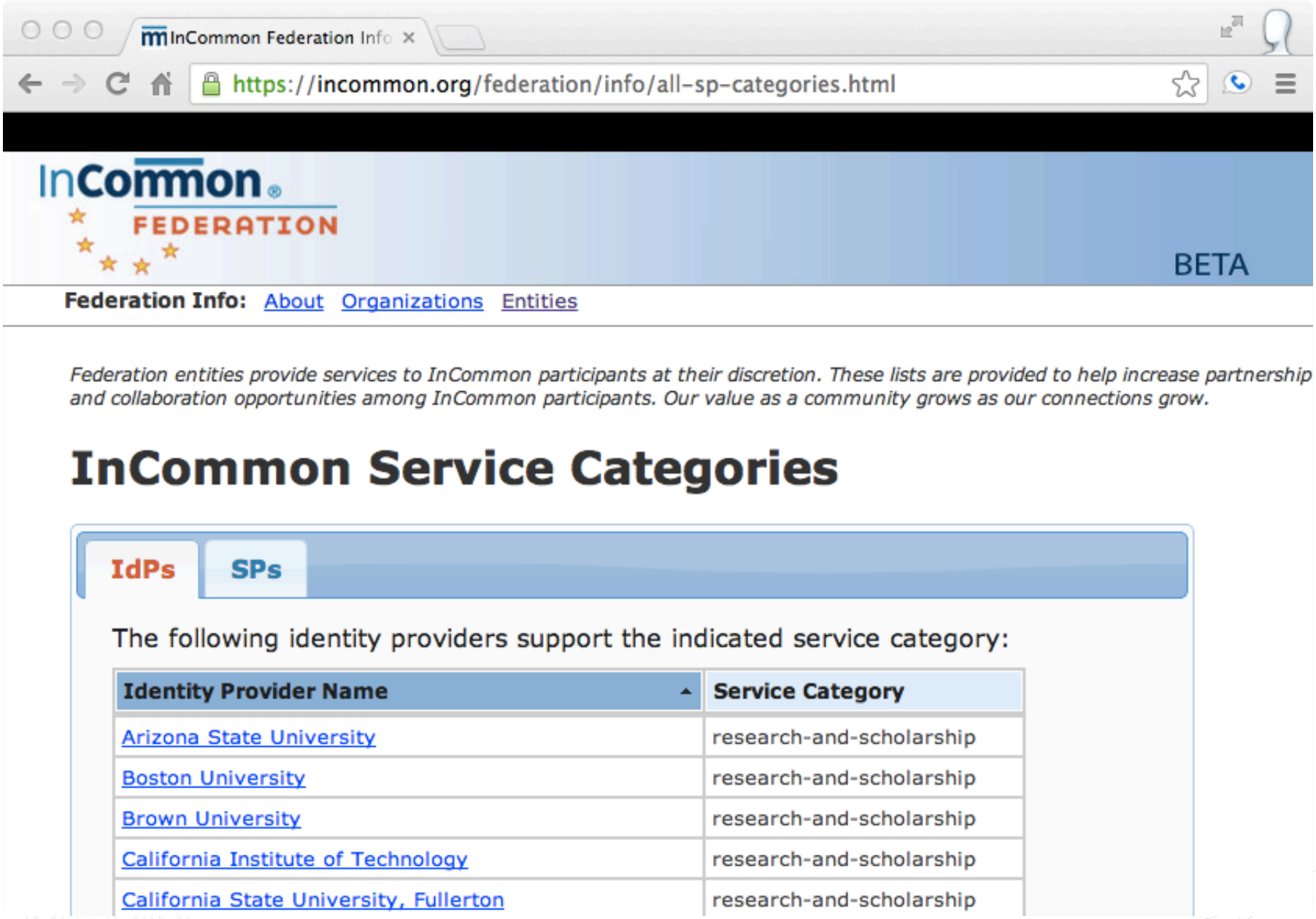
InCommon R&S Category



R&S Tags in InCommon Metadata

```
<EntityDescriptor entityID="https://wiki.ligo.org/shibboleth-sp”>
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute>
        <saml:AttributeValue>
http://id.incommon.org/category/research-and-scholarship
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
```

58 InCommon IdPs



InCommon R&S

"InCommon IdPs are strongly encouraged to release the following attributes to R&S category SPs:

- personal identifiers: email address, person name, eduPersonPrincipalName
- pseudonymous identifier: eduPersonTargetedID
- affiliation: eduPersonScopedAffiliation

where email address refers to the mail attribute and person name refers to displayName and optionally givenName and sn (i.e., surName)."

InCommon R&S

R&S Service Providers must comply with the following requirements:

- The service enhances the research and scholarship activities of some subset of the InCommon community.
- The service meets the following technical requirements:
  - Service metadata has been submitted to InCommon and published in a human-readable format on the InCommon public web site.
  - The SP is a production SAML deployment that supports SAML V2.0 Web Browser SSO.
  - The SP refreshes and verifies metadata at least daily.
  - The SP provides an mdui:DisplayName in metadata (one of numerous User Interface Elements).
  - The SP supports the SAML V2.0 HTTP-POST binding (one of numerous SAML V2.0 endpoints in metadata)
  - The SP provides Technical and Administrative contacts in metadata.
  - The SP provides requested attributes in metadata.

InCommon Assurance

“I can assure you, my intentions are strictly honorable.”

James Bond, Dr. No

InCommon Trust

All participants required to publish POP.

- Participant Operational Practices.
- Details
  - Electronic identity credentials.
  - Electronic identity database.
  - Attribute Assertions.
  - Privacy Policy.
  - Technical standards.
- Available for inspection by other participants.

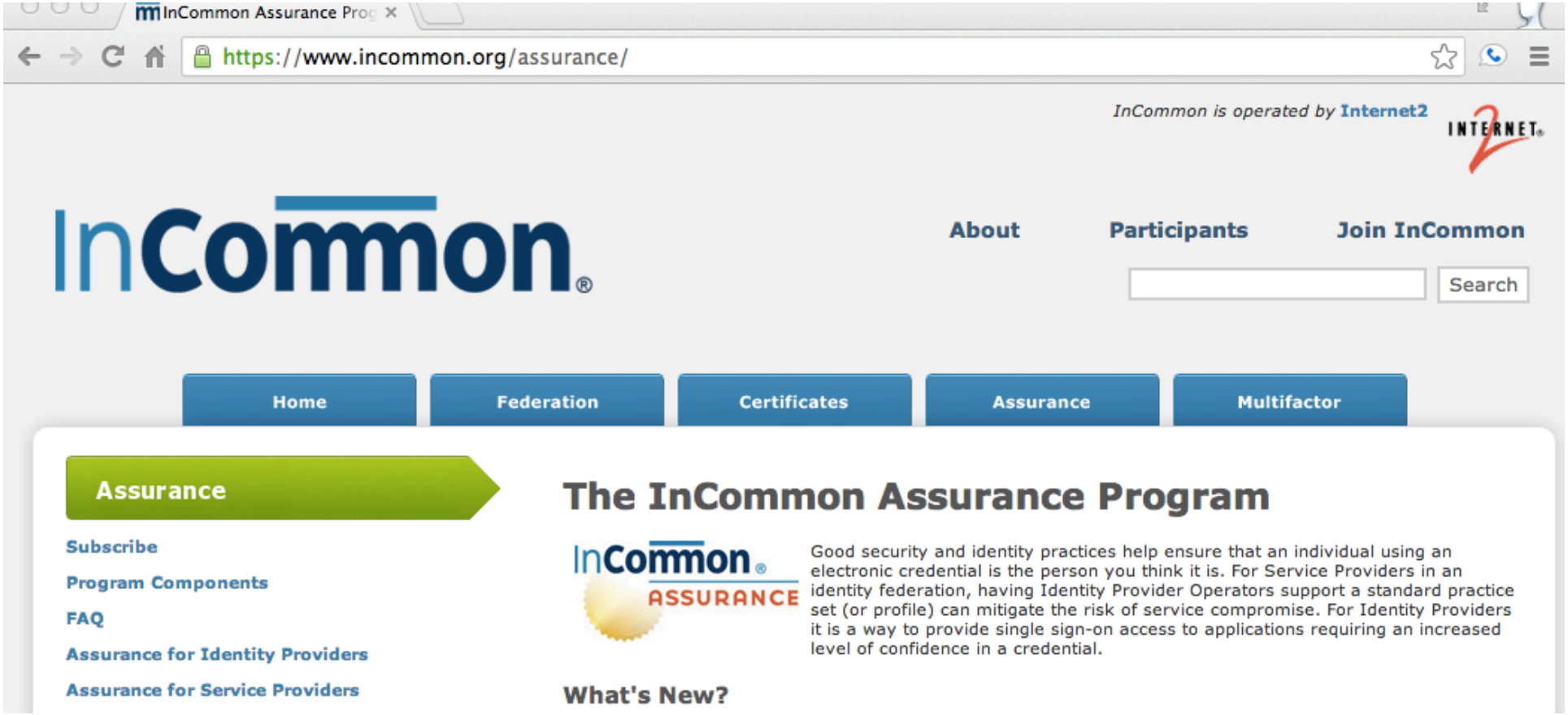
InCommon POP

POP good idea but failed implementation:

- Not all participants have filed a POP.
- Many are > 5 years out of date.
- No framework so level of detail varies.

Hard to measure risk for entire trust fabric based on the current collection of POPs.

InCommon Assurance Program



InCommon Assurance

- Identity Assurance Profiles.
  - IdP operator requirements for registration, credential issuance, technical operations.
  - Bronze and Silver Profiles.
  - Bronze with or without audit, Silver requires audit.
- Identity Assurance Assessment Framework.
  - Background on need for assurance.
  - Defines trust model.
  - Functional model for IdPs.
  - Certification model.
- Informed by but NOT NIST 800-63.
- By Higher Ed and Research for Higher Ed and Research.

InCommon Assurance

- Alternative means.
  - Allows IdPs to petition for alternative mechanism for meeting profile requirements.
  - Intended to provide necessary flexibility.
- Assurance Advisory Committee.
  - Program oversight by community.
  - Reports to steering.
  - Representation by SPs.
  - LIGO representation through 2013.
  - Need more VOs to step up!

InCommon Assurance

Benefits of Assurance

- Increases confidence, reduces risk.
- Getting past passwords—community standards until they are gone.
- It's not NIST 800-63. It's Higher Ed's version.
- Saves time when adding new partners.
- Access to Higher-Value Services like financial and health related.
- Protects your investment — InCommon is an approved Trust Framework Provider under the U.S. Identity, Credential, and Access Management Trust Framework Program.

InCommon Assurance

Substantial investment by InCommon and group of thought leaders.

- Great deal of work by community leaders.
- Well designed and executed so far.

InCommon Assurance

To date one (1) IdP asserts Silver (and Bronze).

- Virginia Tech
- Used alternative means with 2-factor auth.

Slow uptake so far.

- Real costs for campus IdP operators.
  - Staff time.
  - Audit time.
- SP consumers have not arrived.
  - Science VOs could have big impact here.

Beyond InCommon

“You may say I'm a dreamer, but I'm not the only one. I hope someday you'll join us, and the world will be as one.”

John Lennon, Imagine

Beyond InCommon

InCommon gives an SP access to > 300 US IdPs

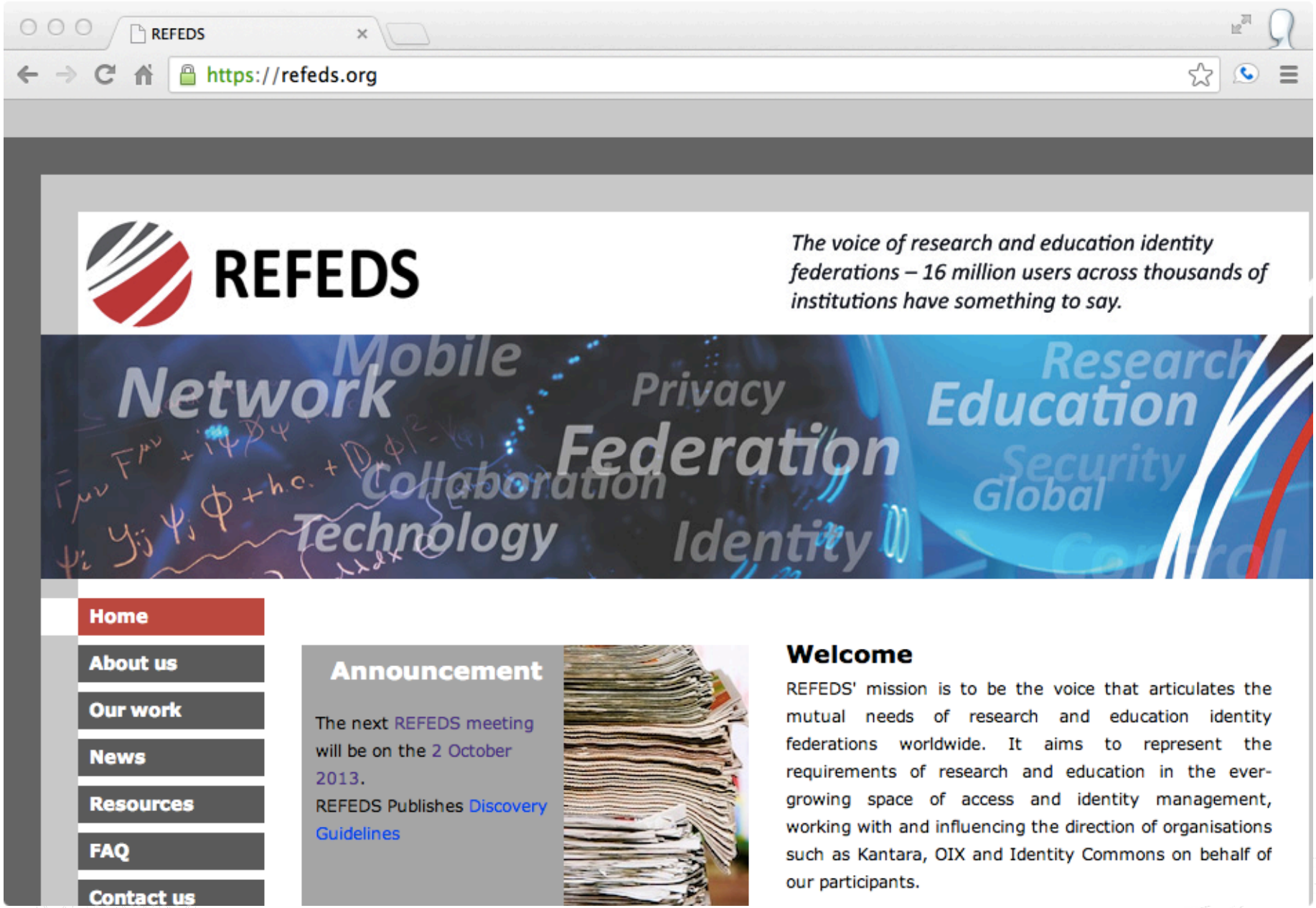
What of the world beyond?

Other SAML Identity Federations

Most European countries, Canada, and Japan have well established SAML identity federations with high coverage in academia and research.

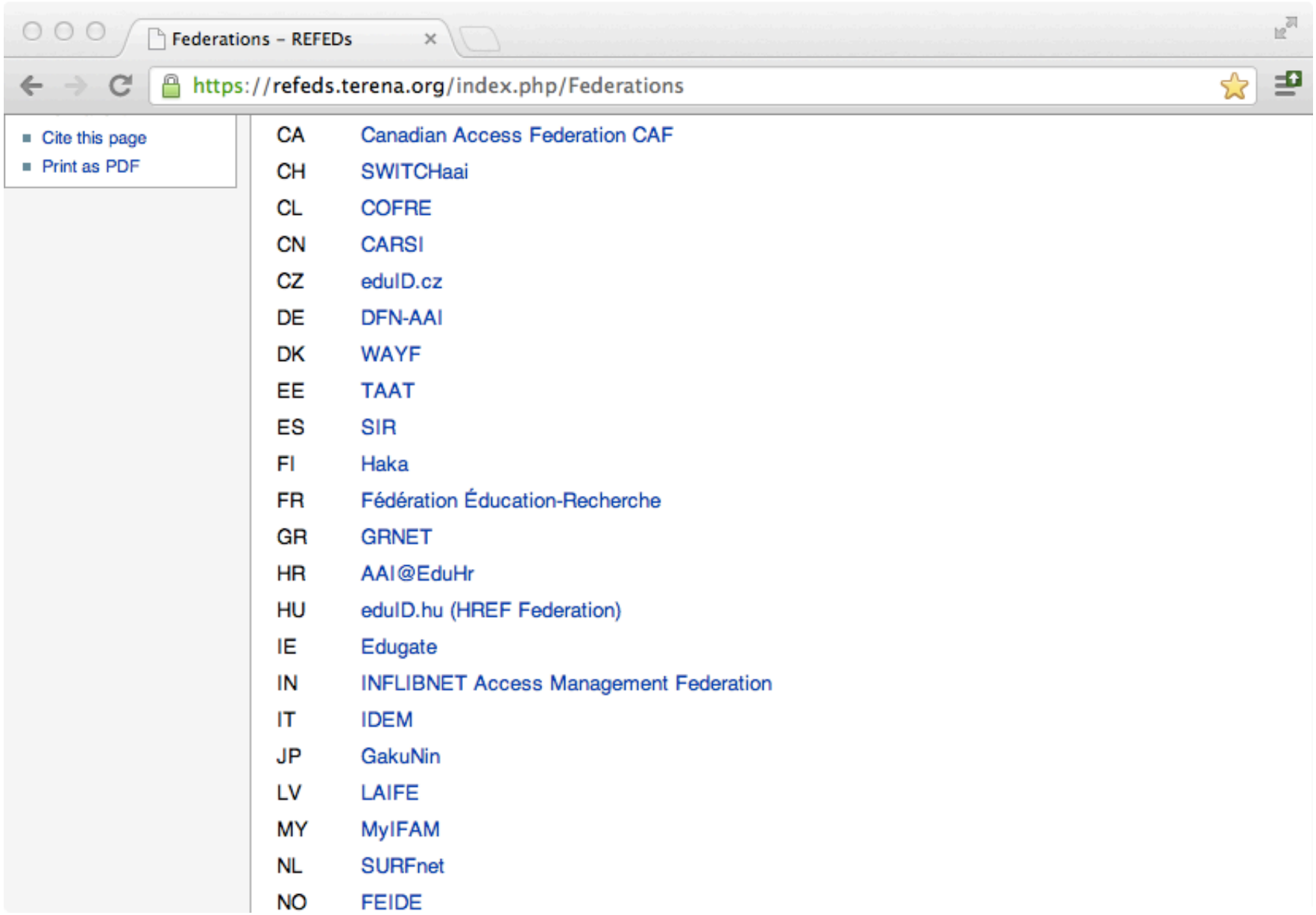
Federations in China, South America, Latin America, and India either newly formed or coming online soon.

REFEDS


REFEDS
https://refeds.org
REFEDS
The voice of research and education identity federations – 16 million users across thousands of institutions have something to say.
Network
Mobile
Privacy
Federation
Collaboration
Technology
Identity
Research
Education
Security
Global
Home
About us
Our work
News
Resources
FAQ
Contact us
Announcement
The next REFEDS meeting will be on the 2 October 2013.
REFEDS Publishes Discovery Guidelines
Welcome
REFEDS' mission is to be the voice that articulates the mutual needs of research and education identity federations worldwide. It aims to represent the requirements of research and education in the ever-growing space of access and identity management, working with and influencing the direction of organisations such as Kantara, OIX and Identity Commons on behalf of our participants.

REFEDS

"The mission of REFEDS is to be the voice that articulates the mutual needs of research and education identity federations worldwide. The group represents the requirements of research and education in the ever-growing space of access and identity management..."


Federations - REFEDs
https://refeds.terena.org/index.php/Federations
Cite this page
Print as PDF
CA Canadian Access Federation CAF
CH SWITCHaai
CL COFRE
CN CARSI
CZ eduID.cz
DE DFN-AAI
DK WAYF
EE TAAT
ES SIR
FI Haka
FR Fédération Éducation-Recherche
GR GRNET
HR AAI@EduHr
HU eduID.hu (HREF Federation)
IE Edugate
IN INFLIBNET Access Management Federation
IT IDEM
JP GakuNin
LV LAIFE
MY MyIFAM
NL SURFnet
NO FEIDE

International Federation

How does a VO interoperate with international relying parties (IdPs or SPs)?

International Federation

Three (3) basic approaches:

1. Point-to-point: negotiate each IdP/SP.
2. Join each relevant national federation.
3. Leverage existing InCommon investment.
   - InCommon pursuing bilateral agreements.
   - InCommon pursuing eduGAIN.

Point-to-point federation

- Usually fastest means to an end.
- Helpful to understand technical challenges.
- Not always an option for IdPs.
- Clearly does not scale.

Joining other Federations

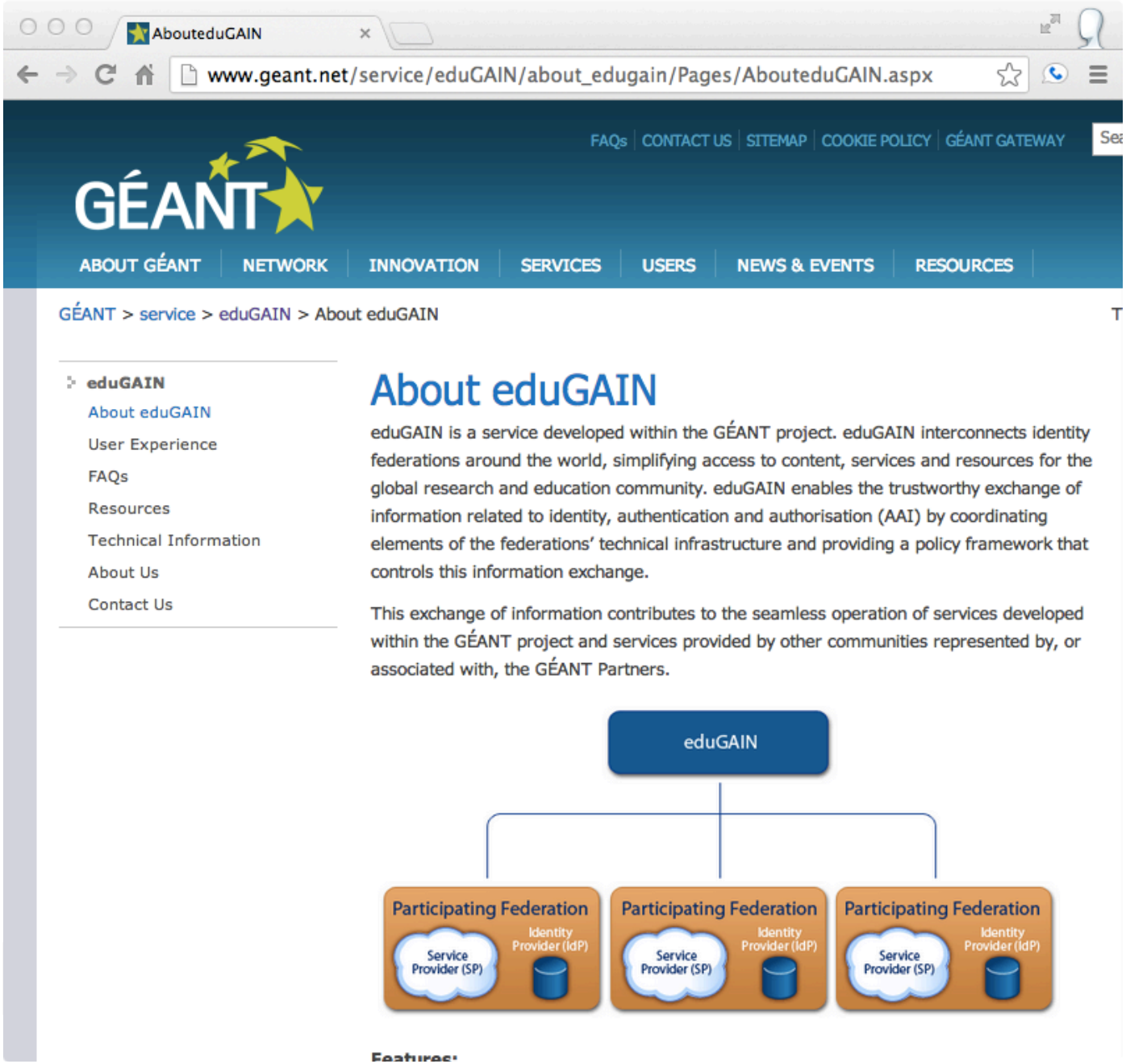
- Spectrum of agreement frameworks varies.
- Some require legal documents.
- Fees vary for VOs.
- Privacy laws further complicate issue.
- Best if targeted at narrow group of IdPs/SPs.

InCommon and Interfederation

InCommon pursuing first bilateral agreement.

- UK Access Federation.
- Large and comprehensive coverage of UK.
- Platform for exploring complicated issues.
  - Are all entities exchanged or some subset?
  - Can there be agreement on attribute release?
  - Can there be agreement on assurance?
- Led by InCommon Interfederation Working Group
  - Chartered by InCommon Technical Advisory Committee.

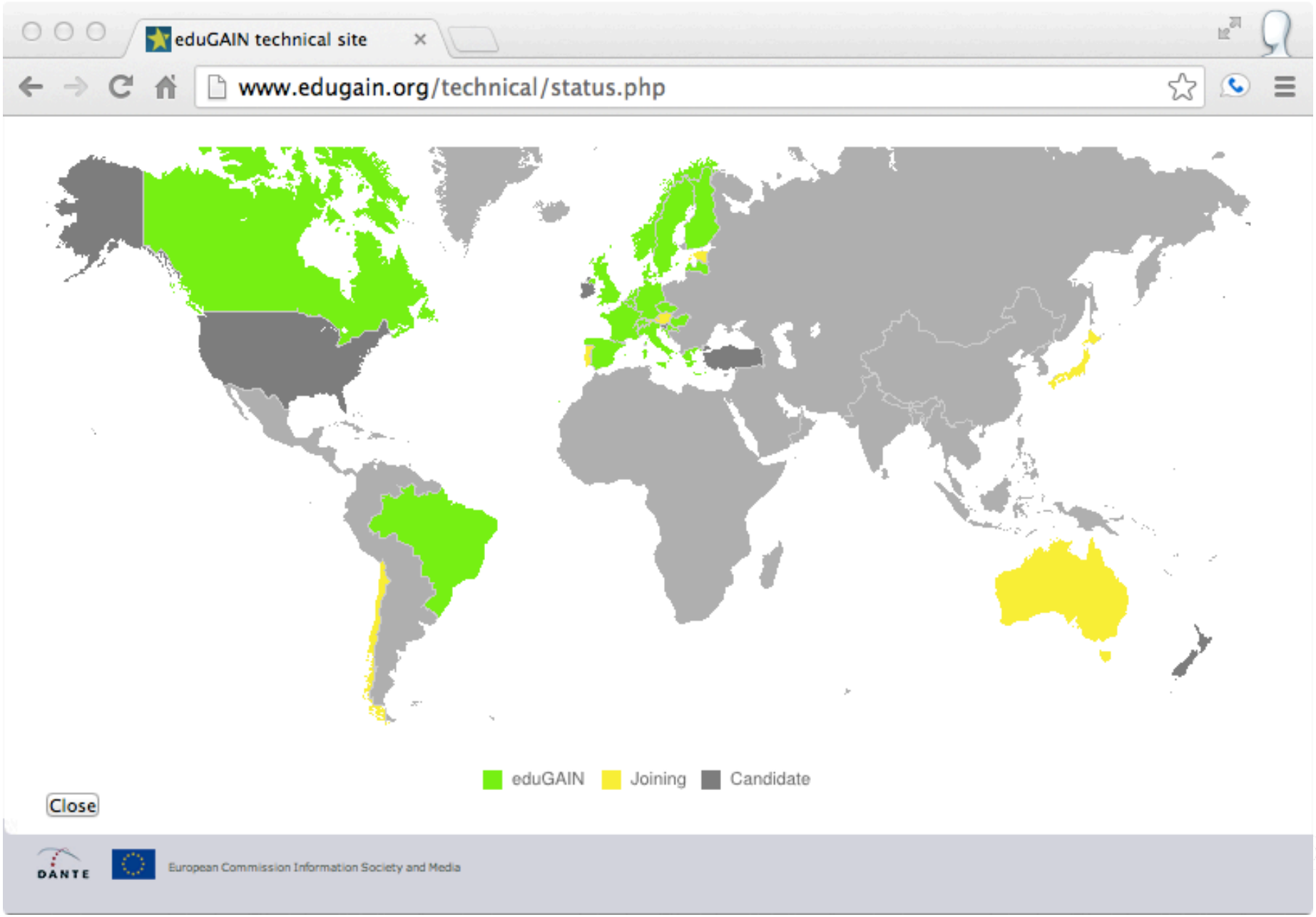
eduGAIN


AbouteduGAIN
www.geant.net/service/eduGAIN/about_edugain/Pages/AbouteduGAIN.aspx
FAQs | CONTACT US | SITEMAP | COOKIE POLICY | GÉANT GATEWAY
GÉANT
ABOUT GÉANT | NETWORK | INNOVATION | SERVICES | USERS | NEWS & EVENTS | RESOURCES
GÉANT > service > eduGAIN > About eduGAIN
eduGAIN
About eduGAIN
User Experience
FAQs
Resources
Technical Information
About Us
Contact Us
About eduGAIN
eduGAIN is a service developed within the GÉANT project. eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.
This exchange of information contributes to the seamless operation of services developed within the GÉANT project and services provided by other communities represented by, or associated with, the GÉANT Partners.
eduGAIN
Participating Federation
Service Provider (SP)
Identity Provider (IdP)
Participating Federation
Service Provider (SP)
Identity Provider (IdP)
Participating Federation
Service Provider (SP)
Identity Provider (IdP)

eduGAIN

“eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations’ technical infrastructure and providing a policy framework that controls this information exchange.”

eduGAIN


eduGAIN technical site
www.edugain.org/technical/status.php
eduGAIN
Joining
Candidate
Close
DANTE
European Commission Information Society and Media

InCommon and eduGAIN

Work underway for InCommon to participate.

- Also led by Interfederation Working Group.
- eduGAIN based on “unilateral declarations”.
- InCommon preparing to declare.
- Possible participation by Q1 2014?

InCommon and eduGAIN

Participation helps but many issues remain.

- Attribute release.
- Attribute categories (R&S?).
- Levels of Assurance.
- No guarantee IdP a VO needs participate.
- VOs needed to help drive use cases.

Application Integration Challenges

“You want answers?”

“I think I’m entitled.”

“You want answers?!”

“I want the truth!”

“You can’t handle the truth!”

A Few Good Men

Application Integration Challenges

Many apps not ready for federated identity.

- Assume a local store for login & password.
- Mix authentication and authorization.
- Assume email is a perfect identifier.
  - Never changes.
  - Never reassigned.
  - Single domain.
- Assume human consumable identifier.
- Built-in weak and coarse grained authz.
- Retrofit can be a lot of work.

LIGO "Domestications"

Done by LIGO

- Foswiki (Twiki)
- Moin
- MediaWiki
- Dokuwiki
- electronic notebook
- document control center
- electronic voting (halo)

Leveraged by LIGO

- Sympa (email)
- Grouper
- Drupal

Application Development Tips

- Expect opaque identifier(s).
  - Use other attributes only if available.
  - Use registration process to collect rest if needed.
- Expect multi-valued attributes.
  - Email addresses.
  - Name identifiers.
  - Need plan for sorting and choosing.

Application Development Tips

- Prepare for multiple IdPs.
  - Users need to choose with IdP to use.
  - Leverage existing IdP discovery service tools.
- Look to consume external authorization.
  - From trusted sources of course.
  - Often VO specific attribute authorities.
- Prepare for more error modes.
  - It's a distributed system after all.
  - Good error handling is harder.

Working Around Attribute Release

What to do if IdP only issues an opaque transient and targeted identifier?

Not much other than negotiate.

If, however, you can get a non-transient and non-targeted identifier...

Working Around Attribute Release

eduPersonPrincipalName

- also called ePPN
- usually persistent
- usually not targeted at one SP
- can be opaque but that can be worked around...
- scott.koranda@ligo.org
  - scoped to ‘ligo.org’

Working Around Attribute Release

If IdP releases ePPN

- Use it as “key” for user into other attributes
- Query attribute authority (AA) for other attributes
  - givenName
  - sn
  - displayName
  - email
- Usually a VO or community specific AA
- AA populated by VO registration process

Working Around Attribute Release

Most VO registration processes not ready for federated identities

- Need mechanism for:
  - enrolling users.
  - Capturing ePPN (or other) during enrollment.
  - Binding other attributes to that ePPN.
  - Grouping identities for authorization (often).

Working Around Attribute Release

Most VO registration processes not ready for federated identities

- Need mechanism for:
  - enrolling users.
  - Capturing ePPN (or other) during enrollment.
  - Binding other attributes to that ePPN.
  - Grouping identities for authorization (often).

Tools Beyond the Web

“Give me a lever long enough and a fulcrum on which to place it, and I shall move the world.

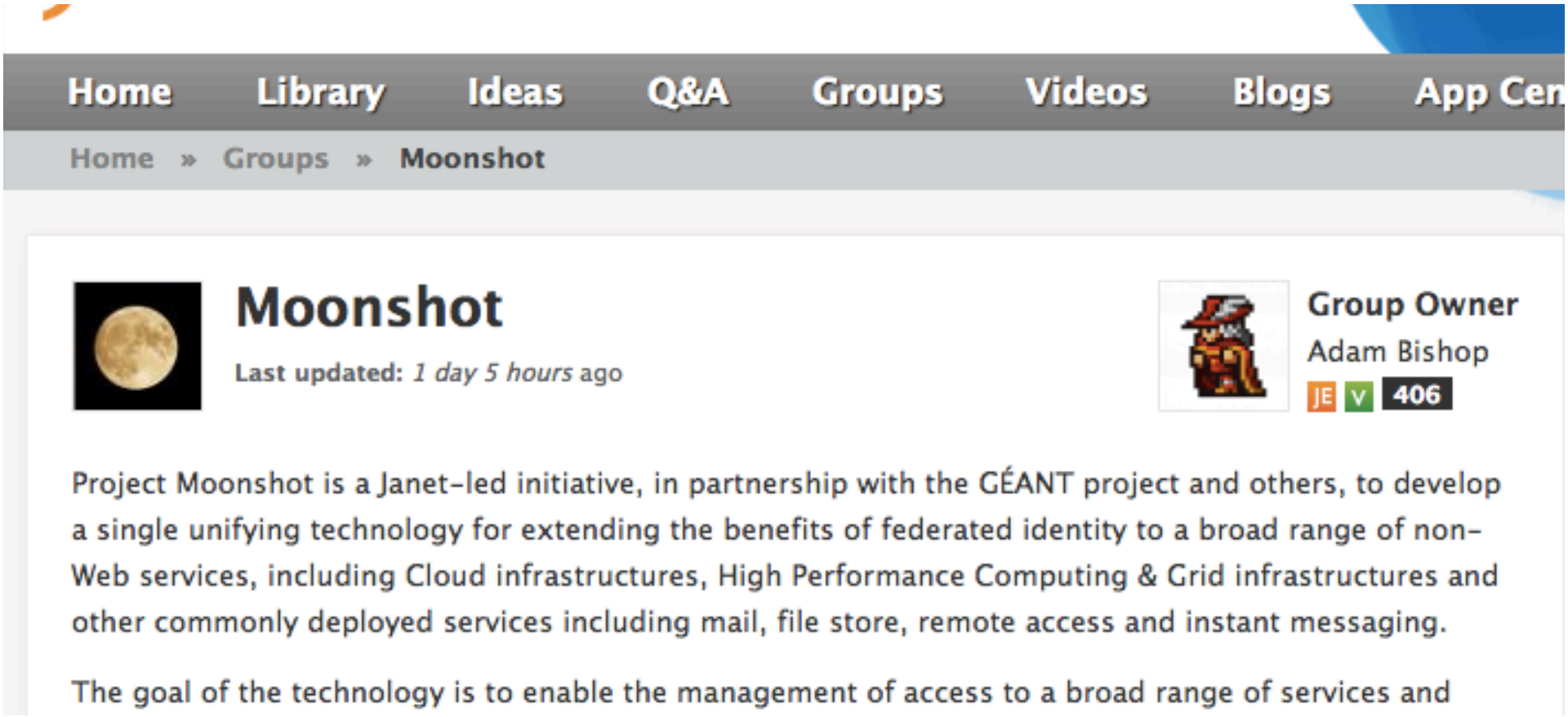
Archimedes

(SAML) Federation Beyond Web

What of the command line?

- Many VO services on ports beyond 80 & 443.
- Existing rich federation known as the “Grid”.
  - International Grid Trust Federation (IGTF).
- What can InCommon and SAML federated identities offer?

Project Moonshot



Project Moonshot

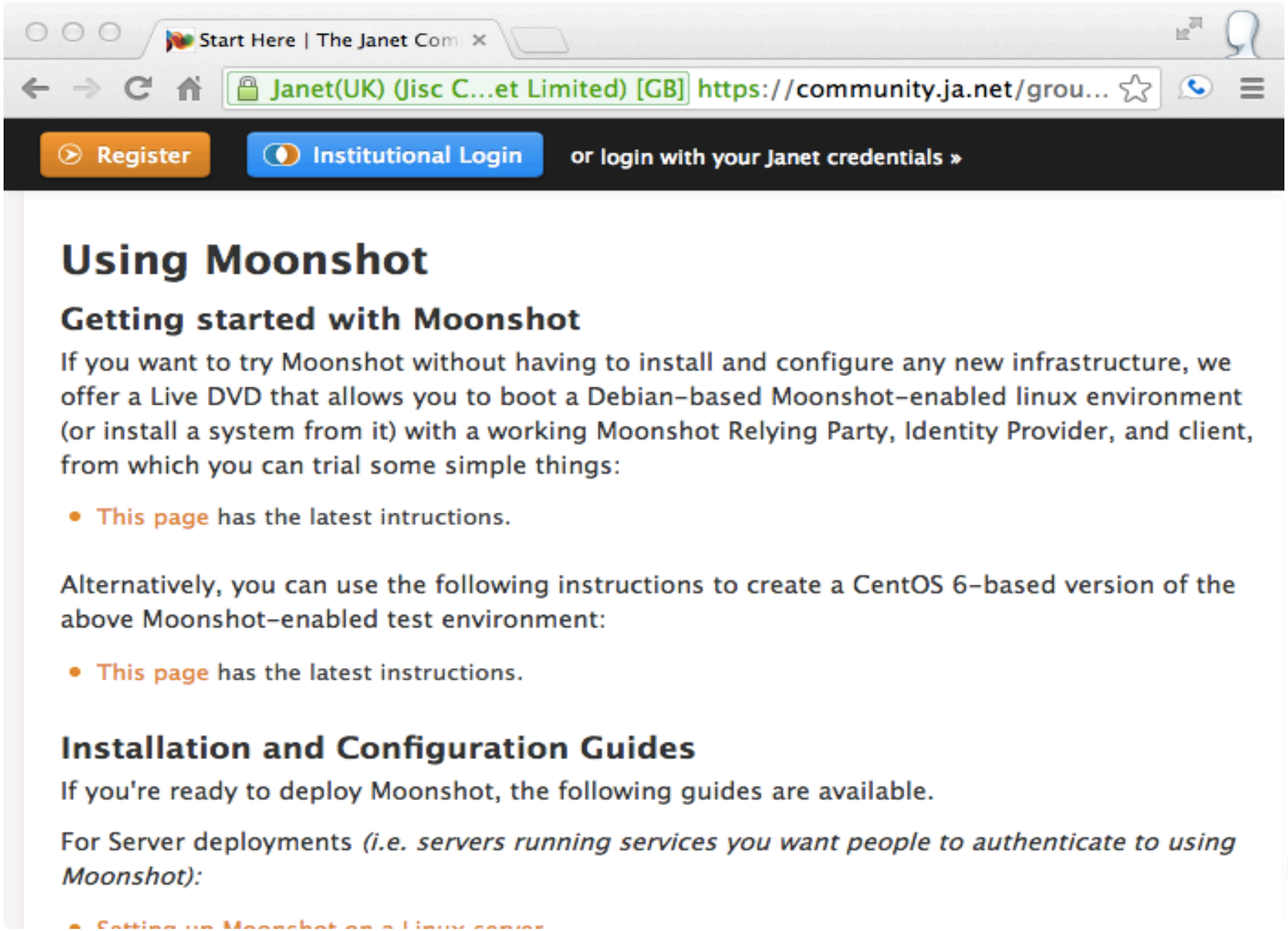
"Project Moonshot is a Janet-led initiative, in partnership with the GÉANT project and others, to develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging."

Project Moonshot

In a nutshell...

- Leverage RADIUS for federation.
- Leverage SAML for attributes and authz.

Large Pilot Project Underway

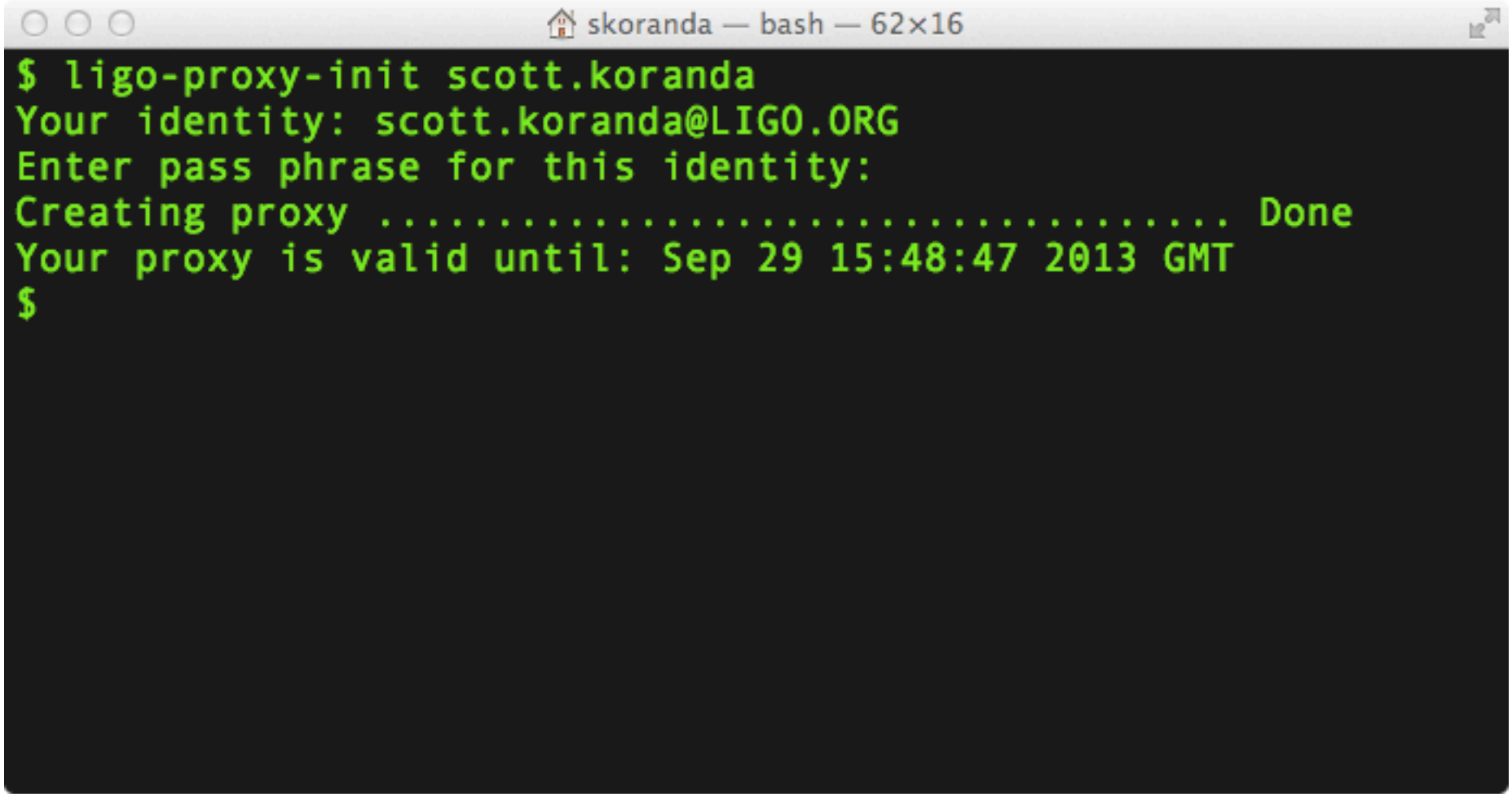


SAML ECP

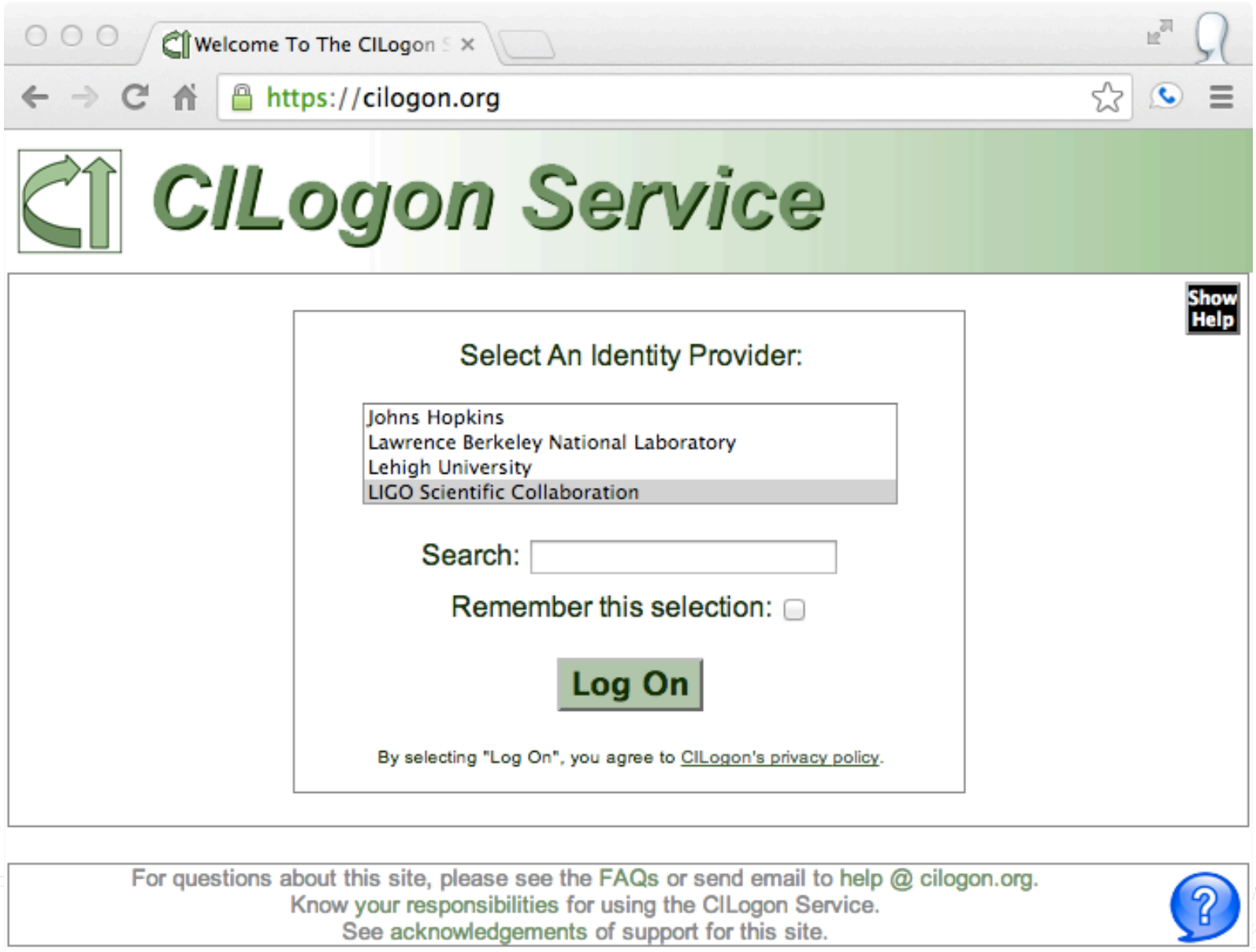
ECP part of SAML2 protocol.

- Enhanced Client or Proxy (ECP).
- Non-browser clients.
- ECP client brokers IdP and SP interaction.
- Usually HTTPS as transport but not necessary.

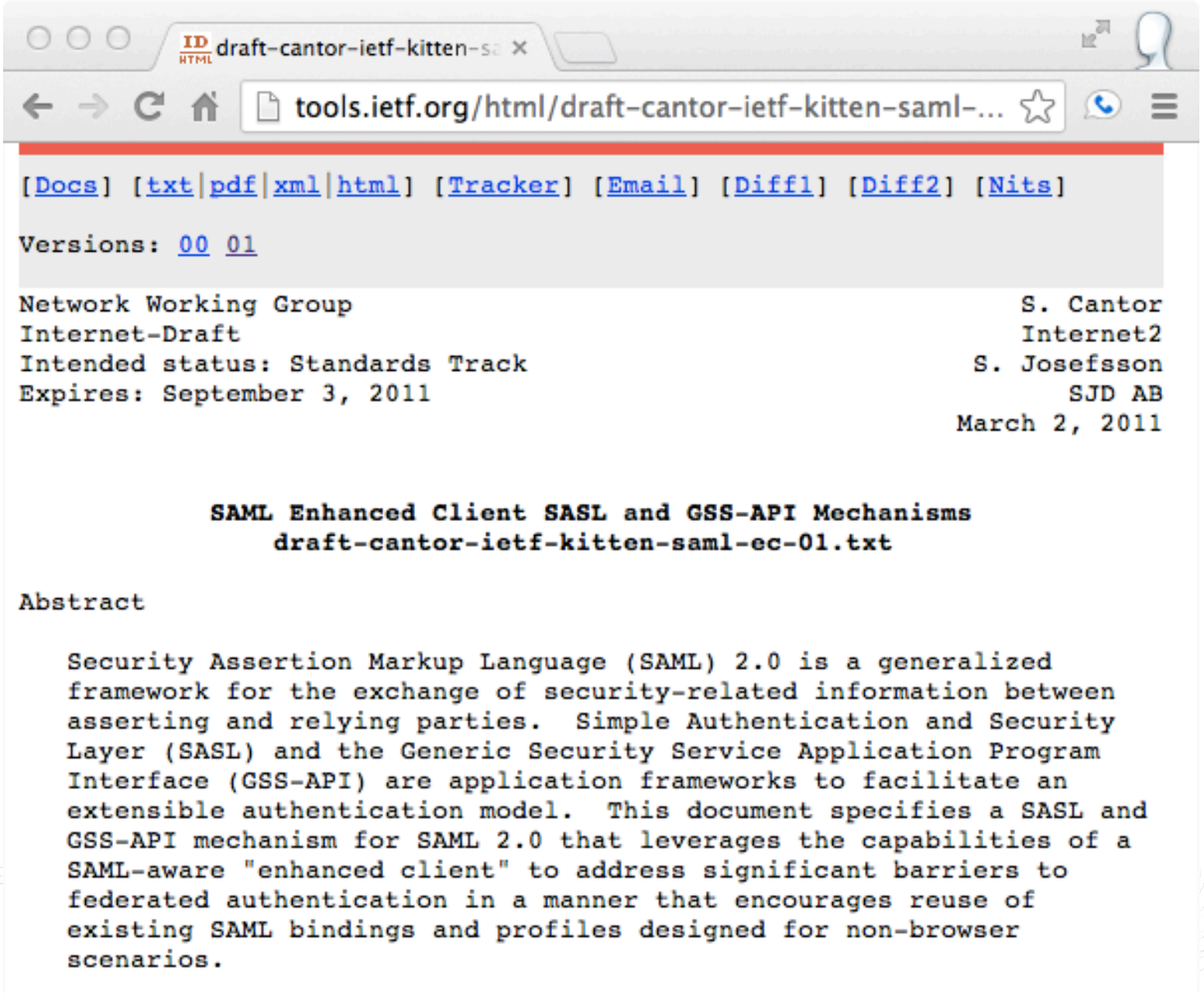
ECP For ligo-proxy-init



CILogon Supports ECP



Nascent GSS-API ECP Effort



draft-cantor-ietf-kitten-s

tools.ietf.org/html/draft-cantor-ietf-kitten-saml-...

[Docs] [txt|pdf|xml|html] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01

Network Working Group — S. Cantor
Internet-Draft — Internet2
Intended status: Standards Track — S. Josefsson
Expires: September 3, 2011 — SJD AB
March 2, 2011

SAML Enhanced Client SASL and GSS-API Mechanisms
draft-cantor-ietf-kitten-saml-ec-01.txt

Abstract

Security Assertion Markup Language (SAML) 2.0 is a generalized framework for the exchange of security-related information between asserting and relying parties. Simple Authentication and Security Layer (SASL) and the Generic Security Service Application Program Interface (GSS-API) are application frameworks to facilitate an extensible authentication model. This document specifies a SASL and GSS-API mechanism for SAML 2.0 that leverages the capabilities of a SAML-aware "enhanced client" to address significant barriers to federated authentication in a manner that encourages reuse of existing SAML bindings and profiles designed for non-browser scenarios.

Thank You

Slides will be made available:

trustedci.org/training

Please complete our short evaluation survey:

http://go.iu.edu/8r6

Breakout group on IAM on day 3, check it out!